

Docket No. 199206US2RD/eam

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takeshi SAITO, et al

SERIAL NO: 09/697,496

FILED: October 27, 2000

FOR: NETWORK CONNECTION DEVICE, NETWORK CONNECTION METHOD, AND COMMUNICATION
DEVICE REALIZING CONTENTS PROTECTION PROCEDURE OVER NETWORKS

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	11-310295	October 29, 1999

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
 - ☐ are submitted herewith
 - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak

Registration No. 24,913

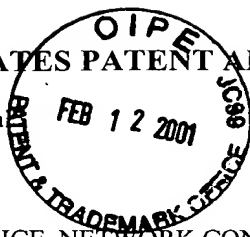
Joseph A. Scafetta, Jr.
Registration No. 26,803



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

2/27/01
JPM



RECEIVED

FEB 14 2001

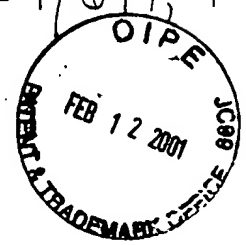
Technology Center 2100

RECEIVED

FEB 14 2001

Technology Center 2100

09/697,496



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1 9 9 9 年 1 0 月 2 9 日

出 願 番 号
Application Number:

平成 1 1 年 特 許 願 第 3 1 0 2 9 5 号

RECEIVED

FEB 14 2001

Technology Center 2100

出 願 人
Applicant (s):

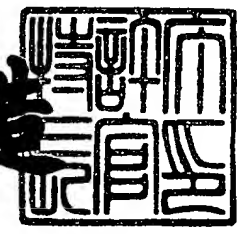
株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 0 年 1 0 月 2 7 日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2 0 0 0 - 3 0 8 7 8 2 7

【書類名】 特許願

【整理番号】 A009905170

【提出日】 平成11年10月29日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/00

【発明の名称】 ネットワーク接続装置、通信装置及びネットワーク接続方法

【請求項の数】 16

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

【氏名】 斉藤 健

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

【氏名】 高島 由彰

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

【氏名】 橋本 幹生

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

特平 11-310295

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク接続装置、通信装置及びネットワーク接続方法

【特許請求の範囲】

【請求項 1】

第 1 の IEEE 1394 バスと第 2 の IEEE 1394 バスとを接続するネットワーク接続装置において、

前記第 1 の IEEE 1394 バス上の第 1 の同期チャンネルまたは第 1 の非同期ストリームチャンネルを介して、前記第 1 の IEEE 1394 バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、

前記データを前記第 2 の IEEE 1394 バス上の第 2 の同期チャンネルまたは第 2 の非同期ストリームチャンネルを介して、前記第 2 の IEEE 1394 バス上に接続された受信ノードに転送するデータ転送手段と、

前記受信ノードから、前記第 2 の IEEE 1394 バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、

前記問い合わせを受信した場合、前記第 1 の IEEE 1394 バス上の所定の packets を介して、前記送信ノードに該情報の問い合わせを行う問い合わせ手段と、

前記送信ノードから、前記第 1 の IEEE 1394 バス上の所定の packets を介して、該情報の問い合わせに対する応答を受信する応答受信手段と、

前記応答を、前記第 2 の IEEE 1394 バス上の所定の packets を介して、前記受信ノードに通知する応答通知手段とを具備したことを特徴とするネットワーク接続装置。

【請求項 2】

前記所定の packets は、同期 packets、非同期ストリーム、非同期 packets のいずれかであることを特徴とする請求項 1 に記載のネットワーク接続装置。

【請求項 3】

前記応答受信手段が受信する前記応答の packets には、前記送信ノードに関す

る情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれることを特徴とする請求項 1 に記載のネットワーク接続装置。

【請求項 4】

前記第 2 の IEEE 1394 バス上の受信ノードは、通知を受けた前記情報に基づいて、前記第 1 の IEEE 1394 バス上の送信ノードとの間で直接、認証・鍵交換手続きを行うものであることを特徴とする請求項 2 または 3 に記載のネットワーク接続装置。

【請求項 5】

第 1 の IEEE 1394 バスと第 2 の IEEE 1394 バスとを接続するネットワーク接続装置において、

前記第 1 の IEEE 1394 バス上の第 1 の同期チャンネルまたは第 1 の非同期ストリームチャンネルを介して、前記第 1 の IEEE 1394 バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、

前記データを前記第 2 の IEEE 1394 バス上の第 2 の同期チャンネルまたは第 2 の非同期ストリームチャンネルを介して、前記第 2 の IEEE 1394 バス上に接続された受信ノードに転送するデータ転送手段と、

前記受信ノードから、前記第 2 の IEEE 1394 バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、

前記問い合わせを受信した場合に、前記第 1 の IEEE 1394 バス上の所定の packets を介して、前記送信ノードに、自装置の仮想的なプラグまたはサブユニットが前記第 1 の同期チャンネルのデータを受信するものであるとして、該情報の問い合わせを行う問い合わせ手段と、

前記送信ノードから、前記第 1 の IEEE 1394 バス上の所定の packets を介して、該情報の問い合わせに対する応答を受信する応答受信手段と、

前記問い合わせを受信した場合に、前記第 2 の IEEE 1394 バス上の所定の packets を介して、前記受信ノードに、自装置の仮想的なプラグまたはサブユニットが前記第 2 の同期チャンネルのデータを送信するものであるとして、該情報

の問い合わせに対する応答を通知する応答通知手段とを具備したことを特徴とするネットワーク接続装置。

【請求項 6】

前記所定のパケットは、同期パケット、非同期ストリーム、非同期パケットのいずれかであることを特徴とする請求項 5 に記載のネットワーク接続装置。

【請求項 7】

前記問い合わせ受信手段が受信する前記問い合わせのパケットには、前記受信ノードに関する情報として、前記受信ノードを識別する情報および前記データの転送のために用いられる前記受信ノードのプラグまたはサブユニットを識別する情報が含まれ、

前記応答受信手段が受信する前記応答のパケットには、前記送信ノードに関する情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれ、

前記ネットワーク接続装置は、

前記第 1 の IEEE 1394 バス上で前記問い合わせに回答した送信ノードのプラグまたはサブユニットと自装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第 1 の認証・鍵交換処理手段と、

自装置の仮想的なプラグまたはサブユニットと前記第 2 の IEEE 1394 バス上の受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第 2 の認証・鍵交換処理手段とを更に具備したことを特徴とする請求項 5 に記載のネットワーク接続装置。

【請求項 8】

前記第 1 の認証・鍵交換処理手段による認証・鍵交換手続きが完了した後に、前記第 1 の IEEE 1394 バス上の送信ノードから、前記仮想的なプラグまたはサブユニットに関する暗号鍵に関する情報を受信する暗号鍵情報受信手段と、

前記第 2 の認証・鍵交換処理手段による認証・鍵交換手続きの少なくとも一部が完了した後に、前記暗号鍵に関する情報を、前記第 2 の IEEE 1394 上の

受信ノードに転送する暗号鍵情報転送手段とを更に具備したことを特徴とする請求項 7 に記載のネットワーク接続装置。

【請求項 9】

前記第 1 の同期チャンネルまたは前記第 1 の非同期ストリームチャンネルを識別する情報と、前記送信ノードを識別する情報と、前記第 2 の同期チャンネルまたは前記第 2 の非同期ストリームチャンネルを識別する情報との対応関係を記憶する記憶手段を更に具備し、

前記問い合わせ手段で受信した情報に含まれる前記第 2 の同期チャンネルまたは前記第 2 の非同期ストリームチャンネルを識別する情報に基づいて、前記記憶手段に記憶された前記対応関係を参照して決定した前記送信ノードに対して前記情報の問い合わせを行うことを特徴とする請求項 1 または 5 に記載のネットワーク接続装置。

【請求項 10】

同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、1 つ以上の暗号鍵を使用する第 1 のネットワークと、同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、同一の暗号鍵を使用し、かつ所定のチャンネルを介してデータの送信及び又は受信を行う第 2 のネットワークとを接続するネットワーク接続装置において、

前記第 1 のネットワーク上に接続されたノードから転送されたデータを受信するデータ受信手段と、

前記データを前記第 2 のネットワーク上の所定のチャンネルを介して、前記第 2 のネットワーク上に接続されたノードに転送するデータ転送手段と、

前記第 2 のネットワーク上に接続されたノードから、認証要求を受信する認証要求受信手段と、

前記認証要求を受信した場合に、前記第 2 のネットワーク上に接続されたノードに、該ノードが受信しているチャンネルを識別する情報を問い合わせる問い合わせ手段と、

前記第 2 のネットワーク上に接続されたノードから、前記情報の問い合わせに対する応答を受信する応答受信手段と、

前記応答受信手段で受信した応答に含まれる情報により特定される前記第 2 のネットワーク上のチャンネルに転送すべきデータを自装置に送信する前記第 1 のネットワーク上に接続されたノードから、該データのための暗号鍵に関する情報を受信する暗号鍵情報受信手段と、

前記暗号鍵に関する情報を、前記第 2 のネットワーク上のノードに転送する暗号鍵情報転送手段とを具備したことを特徴とするネットワーク接続装置。

【請求項 11】

前記応答により特定される前記第 2 のネットワーク上のチャンネルに転送すべきデータを自装置に送信する前記第 1 のネットワーク上に接続されたノードとの間で、認証・鍵交換手続きを行う第 1 の認証・鍵交換処理手段と、

前記応答により特定される前記第 2 のネットワーク上のチャンネルを介して前記データを転送すべき前記第 2 のネットワーク上に接続されたノードとの間で認証・鍵交換手続きを行う第 2 の認証・鍵交換処理手段とを更に具備したことを特徴とする請求項 10 に記載のネットワーク接続装置。

【請求項 12】

第 1 のネットワークと第 2 のネットワークとを接続するネットワーク接続装置において、

自装置と前記第 1 のネットワーク上の任意の装置との間において、暗号管理情報が同一で且つ異なるフローに属するデータの暗号化は異なる暗号鍵で行い、

自装置と前記第 2 のネットワーク上の任意の装置との間において、暗号管理情報を同じくするデータの暗号化は同一の暗号鍵で行うことを特徴とするネットワーク接続装置。

【請求項 13】

自装置と同一の IEEE 1394 バスに接続されたネットワーク接続装置を介して他の IEEE 1394 バス上の送信ノードからのデータを受信する通信装置において、

前記同一の IEEE 1394 バス上の第 1 の同期チャンネルまたは第 1 の非同期ストリームチャンネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、

受信された前記データが暗号化されている場合に、前記同一の I E E E 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、

前記問い合わせを受信した前記ネットワーク接続装置が前記他の I E E E 1 3 9 4 バス上で該情報の問い合わせを行って取得した該情報の問い合わせに対する応答を、前記同一の I E E E 1 3 9 4 バス上の所定の packets を介して該ネットワーク接続装置から受信する応答受信手段と、

前記応答受信手段で受信した前記応答に含まれる情報に基づいて、前記他の I E E E 1 3 9 4 バス上の送信ノードとの間で直接、認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする通信装置。

【請求項 14】

自装置と同一の I E E E 1 3 9 4 バスに接続されたネットワーク接続装置を介して他の I E E E 1 3 9 4 バス上の送信ノードからのデータを受信する通信装置において、

前記同一の I E E E 1 3 9 4 バス上の第 1 の同期チャネルまたは第 1 の非同期ストリームチャネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、

受信された前記データが暗号化されている場合に、前記同一の I E E E 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、

前記問い合わせを受信した前記ネットワーク接続装置から、前記同一の I E E E 1 3 9 4 バス上の所定の packets を介して、該ネットワーク接続装置を送信ノードとする前記送信ノードに関する情報を含む、前記問い合わせに対する応答を受信する通知受信手段と、

前記通知受信手段で受信した前記通知に含まれる情報に基づいて、前記ネットワーク接続装置との間で認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする通信装置。

【請求項 15】

第 1 の I E E E 1 3 9 4 バスと第 2 の I E E E 1 3 9 4 バスとを接続するネッ

トワーク接続方法において、

前記第 1 の IEEE 1 3 9 4 バス上の送信ノードは、暗号化されたデータを前記第 1 の同期チャンネルを介して送信し、

前記ネットワーク接続装置は、前記第 1 の IEEE 1 3 9 4 バス上の第 1 の同期チャンネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第 2 の IEEE 1 3 9 4 バス上の第 2 の同期チャンネルを介して、前記第 2 の IEEE 1 3 9 4 バス上に接続された受信ノードに転送し、

前記受信ノードは、前記第 2 の IEEE 1 3 9 4 バス上の第 2 の同期チャンネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第 2 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、

前記ネットワーク接続装置は、前記受信ノードから、前記第 2 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受信した場合、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに、該情報の問い合わせを行い、

前記送信ノードは、前記ネットワーク接続装置から、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記情報の問い合わせを受信した場合、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該情報の問い合わせに対する応答を送信し、

前記ネットワーク接続装置は、前記送信ノードから、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記情報の問い合わせに対する応答を受信した場合、該応答を、前記第 2 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記受信ノードに通知し、

前記受信ノードは、前記通知に含まれる情報に基づいて、前記送信ノードとの間で、直接認証・鍵交換手続きを行うことを特徴とするネットワーク接続方法。

【請求項 1 6】

第 1 の IEEE 1 3 9 4 バスと第 2 の IEEE 1 3 9 4 バスとを接続するネッ

トワーク接続方法において、

前記第 1 の I E E E 1 3 9 4 バス上の送信ノードは、暗号化されたデータを前記第 1 の同期チャンネルを介して送信し、

前記ネットワーク接続装置は、前記第 1 の I E E E 1 3 9 4 バス上の第 1 の同期チャンネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第 2 の I E E E 1 3 9 4 バス上の第 2 の同期チャンネルを介して、前記第 2 の I E E E 1 3 9 4 バス上に接続された受信ノードに転送し、

前記受信ノードは、前記第 2 の I E E E 1 3 9 4 バス上の第 2 の同期チャンネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第 2 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該受信ノードを識別する情報および該暗号化されたデータの転送のために用いられる該受信ノードのプラグまたはサブユニットを識別する情報を含む、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、

前記ネットワーク接続装置は、前記受信ノードから、前記第 2 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受けた場合、前記第 1 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第 1 の同期チャンネルのデータを受信するものであるとして、該情報の問い合わせを行うとともに、前記第 2 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記受信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第 2 の同期チャンネルのデータを送信するものであるとして、該情報の問い合わせに対する応答を通知し、

前記送信ノードは、前記ネットワーク接続装置から、前記第 1 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記情報の問い合わせを受信した場合、前記第 1 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該送信ノードを識別する情報および前記暗号化されたデータの転送のために用いられる該送信ノードのプラグまたはサブユニットを識別する情報

を含む、該情報の問い合わせに対する応答を送信し、

前記送信ノードのプラグまたはサブユニットと前記ネットワーク接続装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行うとともに、前記ネットワーク接続装置の仮想的なプラグまたはサブユニットと前記受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行うことを特徴とするネットワーク接続方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、IEEE 1394バスや無線ネットワーク等のネットワーク間のデータ転送を中継するネットワーク接続装置及びネットワーク接続方法、並びにIEEE 1394バスや無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【0002】

【従来の技術】

近年、デジタル放送の開始や、デジタル機器の発売等、いわゆる「家庭AV環境のデジタル化」が大きな注目を集めている。デジタルAVデータは、様々な圧縮が可能、マルチメディアデータとしての処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【0003】

しかしながら、このデジタルAV技術には、「コンテンツの不正コピーを行うことが比較的容易である」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビット」のコピーで、元通りの品質の、しかも未来永劫にわたって一切劣化の無い複製を作ることができてしまうため、いわゆる「不正コピー」の問題が発生する。

【0004】

この「不正コピー」を防ぐための技術がいくつか検討されている。その中の1つが、CPTWG（コピープロテクション技術ワーキンググループ）で検討され

ている「1394CPコンテンツ保護システム仕様(1394CP Content Protection System Specification)」である。この技術は、IEEE1394バスに接続されたノード間で、転送するコンテンツ(例えば、MPEGデータ等)について、送受信ノードの間で予め認証手続きを行い、暗号鍵(コンテンツキー)を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外にはコンテンツが読めないようにする技術である。

【0005】

このようにすることにより、認証を行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ(暗号化されているデータ)をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【0006】

【発明が解決しようとする課題】

IEEE1394バスは、「最低速度でも100Mbps」、「網そのものに自動構成認識機能が備わっている」、「QOS転送機能を持つ」等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルAV向けのネットワークとして、デファクトスタンダードの地位を築いている。

【0007】

しかしながら、このようなIEEE1394の特徴ゆえに、「IEEE1394と他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とIEEE1394バスを接続する場合には、無線網や公衆網が100Mbps以上といった高速性を一般には有していないことや、IEEE1394の自動構成認識機能を無線網や公衆網へそのまま拡張するといった方法が簡単にはとれないことから、IEEE1394プロトコルをそのまま無線網や公衆網に拡張するといった方法を使うことはできない。

【0008】

そこで、IEEE 1394 と無線網や公衆網等の他網との間にプロトコル変換ゲートウェイを配置して相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代理サーバの方法等も提案されている。

【0009】

ところが、これらの方法を、前述した 1394 コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術が未だ IEEE 1394 バスについてのみ定められている状況である。このコピープロテクション技術を「IEEE 1394 と他のネットワークを接続するとき」に拡張するための技術は無いのが現状である。

【0010】

また、IEEE 1394 バス同士を接続する場合には、以下の問題点があった。

【0011】

IEEE 1394 バスに接続された送信ノードが、暗号化されたデータを送信する場合は、暗号化されたデータ、送信元のノード ID、送信チャネルの少なくとも 3 つを含んだパケットを送信する。

【0012】

このデータをネットワーク接続装置を介して接続された他の IEEE 1394 バスに接続された受信ノードに送信する場合、次の 2 つのケースが考えられる。第 1 のケースでは、ネットワーク接続装置は、このパケットの送信元を自装置のノード ID に書き換える。この場合、送信ノードと受信ノードが直接認証・鍵交換をすることはできないという問題があった。一方、第 2 のケースでは、ネットワーク接続装置が、送信元のノード ID を書き換えずにデータを転送する。この場合、異なる IEEE 1394 バス上であるため、ノード ID の重複が発生し、正確なデータの転送がなされないという問題があった。

【0013】

従来のコピープロテクション技術は、IEEE 1394 同士を 1394 ブリッジで接続したシステムに拡張するには不十分であった。

【0014】

本発明は、上記事情を考慮してなされたもので、IEEE 1394 バス同士を接続する 1394 ブリッジで接続したネットワークあるいは IEEE 1394 バス同士を他の無線ネットワークで接続するシステムにおいて、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とするネットワーク接続装置、通信装置及びネットワーク接続方法を提供することを目的とする。

【0015】

また、本発明は、コピープロテクション技術を IEEE 1394 のみならず、これと相互接続された他網にも拡張可能なネットワーク接続装置、通信装置及びネットワーク接続方法を提供することを目的とする。

【0016】

【課題を解決するための手段】

本発明（請求項 1）は、第 1 の IEEE 1394 バスと第 2 の IEEE 1394 バスとを接続するネットワーク接続装置において、前記第 1 の IEEE 1394 バス上の第 1 の同期チャネルまたは第 1 の非同期ストリームチャネルを介して、前記第 1 の IEEE 1394 バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、前記データを前記第 2 の IEEE 1394 バス上の第 2 の同期チャネルまたは第 2 の非同期ストリームチャネルを介して、前記第 2 の IEEE 1394 バス上に接続された受信ノードに転送するデータ転送手段と、前記受信ノードから、前記第 2 の IEEE 1394 バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、前記問い合わせを受信した場合、前記第 1 の IEEE 1394 バス上の所定の packets を介して、前記送信ノードに該情報の問い合わせを行う問い合わせ手段と、前記送信ノードから、前記第 1 の IEEE 1394 バス上の所定の packets を介して、該情報の問い合わせに対する応答を受信する応答受信手段と、前記応答を、前記第 2 の IEEE 1394 バス上の所定の packets を介して、前記受信ノードに通知する応答通知手段とを具備したことを特徴とする。

【0017】

好ましくは、前記所定の packets は、同期 packets、非同期ストリーム、非同期 packets のいずれかであるようにしてもよい。

【0018】

好ましくは、前記応答受信手段が受信する前記応答のパケットには、前記送信ノードに関する情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれるようにしてもよい。

【0019】

好ましくは、前記第2のIEEE1394バス上の受信ノードは、通知を受けた前記情報に基づいて、前記第1のIEEE1394バス上の送信ノードとの間で直接、認証・鍵交換手続きを行うものであるようにしてもよい。

【0020】

好ましくは、前記第1の同期チャンネルまたは前記第1の非同期ストリームチャンネルを識別する情報と、前記送信ノードを識別する情報と、前記第2の同期チャンネルまたは前記第2の非同期ストリームチャンネルを識別する情報との対応関係を記憶する記憶手段を更に具備し、前記問い合わせ手段で受信した情報に含まれる前記第2の同期チャンネルまたは前記第2の非同期ストリームチャンネルを識別する情報に基づいて、前記記憶手段に記憶された前記対応関係を参照して決定した前記送信ノードに対して前記情報の問い合わせを行うようにしてもよい。

【0021】

また、本発明（請求項5）は、第1のIEEE1394バスと第2のIEEE1394バスとを接続するネットワーク接続装置において、前記第1のIEEE1394バス上の第1の同期チャンネルまたは第1の非同期ストリームチャンネルを介して、前記第1のIEEE1394バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、前記データを前記第2のIEEE1394バス上の第2の同期チャンネルまたは第2の非同期ストリームチャンネルを介して、前記第2のIEEE1394バス上に接続された受信ノードに転送するデータ転送手段と、前記受信ノードから、前記第2のIEEE1394バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、前記問い合わせを受信した場合に、前記第1のIEEE1394バス上の所定の packets を介して、前記送信ノードに、自装置の仮想的なプ

ラグまたはサブユニットが前記第 1 の同期チャネルのデータを受信するものであるとして、該情報の問い合わせを行う問い合わせ手段と、前記送信ノードから、前記第 1 の I E E E 1 3 9 4 バス上の所定の packets を介して、該情報の問い合わせに対する応答を受信する応答受信手段と、前記問い合わせを受信した場合に、前記第 2 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記受信ノードに、自装置の仮想的なプラグまたはサブユニットが前記第 2 の同期チャネルのデータを送信するものであるとして、該情報の問い合わせに対する応答を通知する応答通知手段とを具備したことを特徴とする。

【 0 0 2 2 】

好ましくは、前記所定の packets は、同期 packets、非同期ストリーム、非同期 packets のいずれかであるようにしてもよい。

【 0 0 2 3 】

好ましくは、前記問い合わせ受信手段が受信する前記問い合わせの packets には、前記受信ノードに関する情報として、前記受信ノードを識別する情報および前記データの転送のために用いられる前記受信ノードのプラグまたはサブユニットを識別する情報が含まれ、前記応答受信手段が受信する前記応答の packets には、前記送信ノードに関する情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれ、前記ネットワーク接続装置は、前記第 1 の I E E E 1 3 9 4 バス上で前記問い合わせに応答した送信ノードのプラグまたはサブユニットと自装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第 1 の認証・鍵交換処理手段と、自装置の仮想的なプラグまたはサブユニットと前記第 2 の I E E E 1 3 9 4 バス上の受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第 2 の認証・鍵交換処理手段とを更に具備するようにしてもよい。

【 0 0 2 4 】

好ましくは、前記第 1 の認証・鍵交換処理手段による認証・鍵交換手続きが完了した後に、前記第 1 の I E E E 1 3 9 4 バス上の送信ノードから、前記仮想的なプラグまたはサブユニットに関係する暗号鍵に関する情報を受信する暗号鍵情

報受信手段と、前記第 2 の認証・鍵交換処理手段による認証・鍵交換手続きの少なくとも一部が完了した後に、前記暗号鍵に関する情報を、前記第 2 の I E E E 1 3 9 4 上の受信ノードに転送する暗号鍵情報転送手段とを更に具備するようにしてもよい。

【 0 0 2 5 】

好ましくは、前記第 1 の同期チャンネルまたは前記第 1 の非同期ストリームチャンネルを識別する情報と、前記送信ノードを識別する情報と、前記第 2 の同期チャンネルまたは前記第 2 の非同期ストリームチャンネルを識別する情報との対応関係を記憶する記憶手段を更に具備し、前記問い合わせ手段で受信した情報に含まれる前記第 2 の同期チャンネルまたは前記第 2 の非同期ストリームチャンネルを識別する情報に基づいて、前記記憶手段に記憶された前記対応関係を参照して決定した前記送信ノードに対して前記情報の問い合わせを行うようにしてもよい。

【 0 0 2 6 】

また、本発明（請求項 1 0）は、同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、1 つ以上の暗号鍵を使用する第 1 のネットワークと、同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、同一の暗号鍵を使用し、かつ所定のチャンネルを介してデータの送信及び又は受信を行う第 2 のネットワークとを接続するネットワーク接続装置において、前記第 1 のネットワーク上に接続されたノードから転送されたデータを受信するデータ受信手段と、前記データを前記第 2 のネットワーク上の所定のチャンネルを介して、前記第 2 のネットワーク上に接続されたノードに転送するデータ転送手段と、前記第 2 のネットワーク上に接続されたノードから、認証要求を受信する認証要求受信手段と、前記認証要求を受信した場合に、前記第 2 のネットワーク上に接続されたノードに、該ノードが受信しているチャンネルを識別する情報を問い合わせる問い合わせ手段と、前記第 2 のネットワーク上に接続されたノードから、前記情報の問い合わせに対する応答を受信する応答受信手段と、前記応答受信手段で受信した応答に含まれる情報により特定される前記第 2 のネットワーク上のチャンネルに転送すべきデータを自装置に送信する前記第 1 のネットワーク上に接続されたノードから、該データのための暗

号鍵に関する情報を受信する暗号鍵情報受信手段と、前記暗号鍵に関する情報を、前記第2のネットワーク上のノードに転送する暗号鍵情報転送手段とを具備したことを特徴とする。

【0027】

好ましくは、前記応答により特定される前記第2のネットワーク上のチャンネルに転送すべきデータを自装置に送信する前記第1のネットワーク上に接続されたノードとの間で、認証・鍵交換手続きを行う第1の認証・鍵交換処理手段と、前記応答により特定される前記第2のネットワーク上のチャンネルを介して前記データを転送すべき前記第2のネットワーク上に接続されたノードとの間で認証・鍵交換手続きを行う第2の認証・鍵交換処理手段とを更に具備するようにしてもよい。

【0028】

また、本発明（請求項12）は、第1のネットワークと第2のネットワークとを接続するネットワーク接続装置において、自装置と前記第1のネットワーク上の任意の装置との間において、暗号管理情報が同一で且異なるフローに属するデータの暗号化は異なる暗号鍵で行い、自装置と前記第2のネットワーク上の任意の装置との間において、暗号管理情報を同じくするデータの暗号化は同一の暗号鍵で行うことを特徴とする。暗号管理情報は、例えば、「このデータは何回コピー可」、「このデータはコピー不可」等、送られるデータのコピーをどの様に扱うかが記載されている情報である。

【0029】

また、本発明（請求項13）は、自装置と同一のIEEE1394バスに接続されたネットワーク接続装置を介して他のIEEE1394バス上の送信ノードからのデータを受信する通信装置において、前記同一のIEEE1394バス上の第1の同期チャンネルまたは第1の非同期ストリームチャンネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、受信された前記データが暗号化されている場合に、前記同一のIEEE1394バス上の所定の packets を介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、前記問い合

わせを受信した前記ネットワーク接続装置が前記他の I E E E 1 3 9 4 バス上で該情報の問い合わせを行って取得した該情報の問い合わせに対する応答を、前記同一の I E E E 1 3 9 4 バス上の所定の packets を介して該ネットワーク接続装置から受信する応答受信手段と、前記応答受信手段で受信した前記応答に含まれる情報に基づいて、前記他の I E E E 1 3 9 4 バス上の送信ノードとの間で直接、認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする。

【0030】

また、本発明（請求項 14）は、自装置と同一の I E E E 1 3 9 4 バスに接続されたネットワーク接続装置を介して他の I E E E 1 3 9 4 バス上の送信ノードからのデータを受信する通信装置において、前記同一の I E E E 1 3 9 4 バス上の第 1 の同期チャンネルまたは第 1 の非同期ストリームチャンネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、受信された前記データが暗号化されている場合に、前記同一の I E E E 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、前記問い合わせを受信した前記ネットワーク接続装置から、前記同一の I E E E 1 3 9 4 バス上の所定の packets を介して、該ネットワーク接続装置を送信ノードとする前記送信ノードに関する情報を含む、前記問い合わせに対する応答を受信する通知受信手段と、前記通知受信手段で受信した前記通知に含まれる情報に基づいて、前記ネットワーク接続装置との間で認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする。

【0031】

また、本発明（請求項 15）は、第 1 の I E E E 1 3 9 4 バスと第 2 の I E E E 1 3 9 4 バスとを接続するネットワーク接続方法において、前記第 1 の I E E E 1 3 9 4 バス上の送信ノードは、暗号化されたデータを前記第 1 の同期チャンネルを介して送信し、前記ネットワーク接続装置は、前記第 1 の I E E E 1 3 9 4 バス上の第 1 の同期チャンネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第 2 の I E E E 1 3 9 4 バス上

の第 2 の同期チャネルを介して、前記第 2 の IEEE 1 3 9 4 バス上に接続された受信ノードに転送し、前記受信ノードは、前記第 2 の IEEE 1 3 9 4 バス上の第 2 の同期チャネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第 2 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、前記ネットワーク接続装置は、前記受信ノードから、前記第 2 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受信した場合、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに、該情報の問い合わせを行い、前記送信ノードは、前記ネットワーク接続装置から、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記情報の問い合わせを受信した場合、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該情報の問い合わせに対する応答を送信し、前記ネットワーク接続装置は、前記送信ノードから、前記第 1 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記情報の問い合わせに対する応答を受信した場合、該応答を、前記第 2 の IEEE 1 3 9 4 バス上の所定の packets を介して、前記受信ノードに通知し、前記受信ノードは、前記通知に含まれる情報に基づいて、前記送信ノードとの間で、直接認証・鍵交換手続きを行うことを特徴とする。

【 0 0 3 2 】

また、本発明（請求項 1 6）は、第 1 の IEEE 1 3 9 4 バスと第 2 の IEEE 1 3 9 4 バスとを接続するネットワーク接続方法において、前記第 1 の IEEE 1 3 9 4 バス上の送信ノードは、暗号化されたデータを前記第 1 の同期チャネルを介して送信し、前記ネットワーク接続装置は、前記第 1 の IEEE 1 3 9 4 バス上の第 1 の同期チャネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第 2 の IEEE 1 3 9 4 バス上の第 2 の同期チャネルを介して、前記第 2 の IEEE 1 3 9 4 バス上に接続された受信ノードに転送し、前記受信ノードは、前記第 2 の IEEE 1 3 9 4 バス上の第 2 の同期チャネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第 2 の IEEE 1 3 9 4 バス上の所定の packets

を介して、前記ネットワーク接続装置に、該受信ノードを識別する情報および該暗号化されたデータの転送のために用いられる該受信ノードのプラグまたはサブユニットを識別する情報を含む、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、前記ネットワーク接続装置は、前記受信ノードから、前記第 2 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに関する情報の問い合わせを受けた場合、前記第 1 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記送信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第 1 の同期チャネルのデータを受信するものであるとして、該情報の問い合わせを行うとともに、前記第 2 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記受信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第 2 の同期チャネルのデータを送信するものであるとして、該情報の問い合わせに対する応答を通知し、前記送信ノードは、前記ネットワーク接続装置から、前記第 1 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記情報の問い合わせを受信した場合、前記第 1 の I E E E 1 3 9 4 バス上の所定の packets を介して、前記ネットワーク接続装置に、該送信ノードを識別する情報および前記暗号化されたデータの転送のために用いられる該送信ノードのプラグまたはサブユニットを識別する情報を含む、該情報の問い合わせに対する応答を送信し、前記送信ノードのプラグまたはサブユニットと前記ネットワーク接続装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行うとともに、前記ネットワーク接続装置の仮想的なプラグまたはサブユニットと前記受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行うことを特徴とする。

【 0 0 3 3 】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【 0 0 3 4 】

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させ

るための) プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0035】

本発明(請求項1等)によれば、ネットワーク接続装置が、第2のIEEE1394バス上の受信ノードに、第1のIEEE1394バス上の送信ノードに関する情報を通知してあげるので、受信ノードはネットワークの異なる送信ノードとの間で直接、認証・鍵交換手続きを行うことができ、同じネットワークには接続されていない送受信ノード間のコンテンツ保護手続きが可能となる。

【0036】

また、本発明(請求項5等)によれば、認証問い合わせ手続きにおいて、ネットワーク接続装置が、第1のIEEE1394バス上の送信ノード/第2のIEEE1394バス上の受信ノードにそれぞれ自装置を受信ノード/送信ノードとして通知し、認証・鍵交換手続きについて、ネットワーク接続装置が、第1のIEEE1394バス上の送信ノードとの間および第2のIEEE1394バス上の受信ノードとの間でそれぞれ行い、鍵に関する情報については、送信ノードから受信ノードにフォワードするので、同じネットワークには接続されていない送受信ノード間のコンテンツ保護手続きが可能となる。

【0037】

また、本発明(請求項10等)によれば、ネットワーク接続装置は、第2のネットワーク上の受信ノードから認証要求を受信した場合に、該受信ノードが受信している同期チャネルを確認し、その同期チャネルに転送すべきデータを第1のネットワーク上で送信するノードから該データのための暗号鍵に関する情報を通知された場合、これを第2のネットワーク上の受信ノードに通知するので、同じネットワークには接続されていない送受信ノード間のコンテンツ保護手続きが可能となる。

【0038】

また、本発明では、ネットワーク接続装置は暗号化されたデータを復号化することなくフォワードすることができるため、ネットワーク接続装置を通過する毎に暗号の復号化および再暗号化を行う必要がなくなり、大幅な処理コストの低減

を図ることができる。

【 0 0 3 9 】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【 0 0 4 0 】

(第 1 の実施形態)

図 1 に、本発明を適用するネットワークの全体構成の一例を示す。

【 0 0 4 1 】

本実施形態においては図 1 のネットワークに例示するように、2つの IEEE 1394 バス 104, 105 が中継装置（もしくはネットワーク中継装置）102 によりブリッジ接続されているネットワークにおいて、第 1 の IEEE 1394 バス（104）に接続された送信装置 101 から中継装置 102 を介して第 2 の IEEE 1394 バス（105）に接続された受信装置 103 に対して、AV ストリームを転送する場合を例にとって説明する。その際に、その著作権保護（不正コピーの防止）のために、送信ノード（101）と受信ノード（103）との間で転送される AV ストリームは暗号化される場合を考える。また、上記 AV ストリームの一例として MPEG 映像データを用いて説明する。

【 0 0 4 2 】

本実施形態では、IEEE 1394 バス上での認証・鍵交換は、AV データフロー毎あるいは AV/C のプラグ毎に行われ、同じノード間でフロー毎あるいはプラグ毎に異なる暗号鍵 K を使用することが可能であるものとする。ここで、PCR（プラグコントロールレジスタ、iPCR（入力プラグコントロールレジスタ）や oPCR（出力プラグコントロールレジスタ））は、IEEE 1394 AV/C スペックにて規定される論理的な番号であり、ネットワークインタフェース（本実施形態の場合、IEEE 1394 I/F）から入力または出力される AV ストリームデータを入力または出力する入口番号または出口番号と考えればよい。なお、以下で使う具体的な PCR の番号は一例である。

【 0 0 4 3 】

第 1 の IEEE 1394 バス（104）のバス ID を“A”、第 2 の IEEE

1394バス(105)のバスIDを“B”とする。

送信装置101の物理IDを“a”、受信装置103の物理IDを“d”とする。

ノードのノードID(アドレス)は、(バスID、物理ID)で定義される。

送信装置101のノードIDは(A, a)、受信装置103のノードIDは(B, d)で表される。

中継装置102の第1のIEEE1394(104)側のインタフェースのノードIDを(A, b)、中継装置102の第2のIEEE1394(105)側のインタフェースのノードIDを(B, c)とする。

【0044】

なお、本実施形態では、本例において送信側となるノードを送信装置、本例において受信側となるノードを受信装置と呼んでいるが、もちろん、送信装置101や受信装置103は、後述する送信側としての機能や受信側としての機能以外の機能を持っても良いし(送信側としての機能と受信側としての機能の両方の機能を持っても良い)、また、図1では、3つのノード101, 102, 103のみを示してあるが、これらの他にもノードが接続されていてももちろんよい(この点は、後述する他の実施形態においても同様である)。

【0045】

図2に、送信装置101の内部構成例を示す。

【0046】

送信装置101は、図2に示されるように、IEEE1394インタフェース201、AV/C(AV/C Digital Interface Command Set General Specification)プロトコルの処理を行う、AV/Cプロトコル処理部202、AV/Cプロトコル内のコピープロテクションに関する処理を行う、コピープロテクション処理部203、IEEE1394を通して送受信されるデータのうち同期チャンネルを通してやり取りされるデータについて送受信する、ISO信号送受信部204、MPEG映像のストレージである、MPEGストレージ部206、コピープロテクション処理部

2 0 3 から暗号鍵 K を貰い M P E G 映像を暗号化して I S O 信号送受信部 2 0 4 に送出する、暗号化部 2 0 5 を有する。

【 0 0 4 7 】

送信装置 1 0 1 は、M P E G 映像データを蓄積可能なノードであり、要求に応じて M P E G 映像データを送出する。その際、転送経路上で不法にコピーをされることを未然に防止するために必要な場合には送出する M P E G 映像データを暗号化して送出する機能を持つ。そのため、自装置が送出する M P E G 映像データを受信するノードとの間で認証データや暗号鍵等の交換を行うための機構も持つ。

【 0 0 4 8 】

本例では、送信装置 1 0 1 は、受信装置 1 0 3 との間で A V ストリームのやり取りを暗号化を施した上で行うために直接的には中継装置 1 0 2 との間で、間接的に受信装置 1 0 3 との間で、認証・鍵交換手続きを行う。このための認証・鍵交換手続きを行うのが認証のための機器証明（認証フォーマット）A c e r t を内部に持つコピープロテクション処理部 2 0 3 である。

【 0 0 4 9 】

I E E E 1 3 9 4 の場合は、認証・鍵交換の手続きは A V / C プロトコルに含まれるため、A V / C プロトコル処理部 2 0 2 にて多重化処理が行われ、I E E E 1 3 9 4 インタフェース（I / F）2 0 1 を通してパケットのやり取りがなされる。コピープロテクション処理部 2 0 3 にて、使用する暗号鍵 K が決まる。

【 0 0 5 0 】

ここでは、送信装置 1 0 1 から送出される A V ストリームが、M P E G ストリームであるとする。M P E G ストレージ部 2 0 6 から送出された M P E G ストリームは、暗号化部 2 0 5 で暗号鍵 K にて暗号化され、I S O 信号送受信部 2 0 4 で I E E E 1 3 9 4 向けのパケット化やタイムスタンプ処理などがなされ、I E E E 1 3 9 4 インタフェース 2 0 1 を通して第 1 の I E E E 1 3 9 4 バス（1 0 4）に対して送出される。

【 0 0 5 1 】

図 3 に、受信装置 1 0 3 の内部構成例を示す。

【0052】

受信装置103は、図3に示されるように、IEEE1394インタフェース301、AV/Cプロトコルの処理を行う、AV/Cプロトコル処理部302、AV/Cプロトコル内のコピープロテクションに関する処理を行う、コピープロテクション処理部303、IEEE1394を通して送受信されるデータのうち同期チャンネルを通してやり取りされるデータについて送受信する、ISO信号送受信部304、受信した暗号化されたストリーム（MP EG映像等）をコピープロテクション処理部303から渡される暗号鍵Kを使ってこれを復号化する、暗号復号化部305、MP EGデコード部306、映像を表示する、ディスプレイ部307を有する。

【0053】

受信装置103は、受信したMP EG映像データをデコードし表示する機能を有する装置である。その際、転送経路上で不法にコピーをされることを未然に防止するために送信側が暗号化して送出したMP EG映像データを復号化する機能を持つ。そのため、MP EG映像データを送信するノードとの間で認証データや暗号鍵等の交換を行うための機構も持つ。

【0054】

本例では、受信装置103は、送信装置101との間でAVストリームのやり取りを暗号化を施した上で行うために直接的には中継装置102との間で、間接的に送信装置101との間で、認証・鍵交換手続きを行う。このための認証・鍵交換手続きを行うのが認証のための機器証明B c e r tを内部に持つコピープロテクション処理部303である。なお、機器証明B c e r tの発行機関は、送信装置101の機器証明A c e r tの発行機関と同一の発行機関であるものとする。

【0055】

IEEE1394インタフェース（I/F）301を通してパケットを受信すると、コピープロテクションのための認証・鍵交換のためのパケットは、AV/Cプロトコル処理部302にて分離処理が行われ、コピープロテクション処理部303に渡される。この認証・鍵交換の手続きにより、AVストリームの暗号化

に使用される暗号鍵Kが決まる。

【0056】

IEEE1394 インタフェース301を通して暗号化されたAVストリームを受信すると、ISO信号送受信部304にて1394ヘッダの除去やタイムスタンプを用いた同期処理等が行われ、暗号化AVストリームが暗号復号化部305に渡される。コピープロテクション処理部303から暗号鍵Kを貰い、これを復号して、MPEGデコード部306でデコードし、これをディスプレイ部307で映像・音声として表示する。

【0057】

図4に、中継装置102の内部構成例を示す。

【0058】

中継装置102は、図4に示されるように、第1のIEEE1394インタフェース(I/F)401、第2のIEEE1394インタフェース(I/F)408、第1のAV/Cプロトコル処理部402、第2のAV/Cプロトコル処理部409、第1のコピープロテクション処理部403、第2のコピープロテクション処理部410、ブリッジテーブル部405、第1のISO信号送受信部404、第2のISO信号送受信部407、ブリッジ接続処理部406を有する。

【0059】

第1のコピープロテクション処理部403は、第1のIEEE1394バス(104)上の装置(本例の場合、送信装置101)と認証・鍵交換手続きを行う。同様に、第2のコピープロテクション部410は、第2のIEEE1394バス(105)上の装置(本例の場合、受信装置103)と認証・鍵交換手続きを行う。

【0060】

IEEE1394のブリッジ接続においては、複数のIEEE1394バス間の同期チャンネルを接続することが可能となる。この対応関係を記憶するのが、ブリッジテーブル部405である。

【0061】

図5に、ブリッジテーブル部405が管理するブリッジテーブルの構成例を示

す。ブリッジテーブルには、この例では、第1のIEEE1394バス(104)上の特定の同期チャンネル(例えば、#x)と第2のIEEE1394バス(105)上の特定の同期チャンネル(例えば、#y)との間の関係、すなわち、同期チャンネル番号、どちらが送信側でどちらが受信側かを示す情報(送受信の方向)、送信者のノードID=(バスID、物理ID)、それぞれのチャンネルに関して認証・鍵交換を行う認証先等が登録される。後述するように、これらの登録は順次行われていく。

【0062】

次に、実際のコピープロテクションを施した上でのMPEG映像転送のための全体的なシーケンスについて、図6(全体のシーケンス例)、図7(中継装置102のフローチャート例)を参照しながら説明する。

【0063】

まず、送信装置101が、受信装置103に対してAV/Cコマンドを発行し、そのプラグの操作を行う(S501)。具体的には、受信装置103の入力プラグコントロールレジスタ(iPCR)を操作し、例えば、「iPCR[0]を通してデータを受信する旨の要求」あるいは「ディスプレイサブユニットに対する映像表示要求」などのコマンドを発行する。なお、サブユニットは、AV/Cプロトコルにて規定されるノード内の機能要素である。

【0064】

次に、送信装置101は、自装置から受信装置103に至る同期チャンネルの確立を行うため、ブリッジ接続コマンドを発行する(S502)。

【0065】

このブリッジ接続コマンドは、例えば「受信ノード(B, d)のiPCR[0]に至る同期チャンネルを確立せよ。帯域はBW、第1のIEEE1394バス上の同期チャンネル番号は#xを使用すること。」という内容を要求する情報を含む。このコマンドは、非同期パケットの形(例えば、受信装置103宛または中継装置102宛であり、さらにその特定のレジスタ宛になっていてもよい)で送信されても、非同期ストリームの形で送信されてもよいが、どちらの場合も中継装置102により一旦受信される。

【0066】

なお、第1のIEEE1394バス(104)上に、中継装置102以外の中継装置が接続されていても、あるいはこのコマンドが受信されてもよいが、受信装置103に至る経路以外の中継装置は、このコマンドの処理は行わないものとする。

【0067】

送信装置101から送信されたブリッジ接続コマンドは、中継装置102により受信(S701)される(そのブリッジ接続処理部406に渡される)。

【0068】

このブリッジ接続コマンドを受信した中継装置102は、受信ノード(B, d)に至る経路上に自分がいることを認識すると、受信装置103に至る経路(第2のIEEE1394バス)の必要帯域BWをもった同期チャンネル(#y)を確保し、ブリッジ接続コマンドを発行する(S503, S702, S704)。このブリッジ接続コマンドは、受信装置103宛の非同期パケットでもよい。このコマンドの中身は、記録されている同期チャンネル番号が第2のIEEE1394バス上で使用される#yに書き換えられている以外は、S502におけるブリッジ接続コマンドとほぼ同様である。

【0069】

上記コマンドの発行とともに(同時にもしくは相前後して)、ブリッジ接続処理部406は、図5のブリッジテーブルの「同期チャンネル番号」の行と「送受信の方向」の行の値の設定を行う(S703)。このときのブリッジテーブルの登録内容が図5(a)である。

【0070】

これらブリッジ接続コマンドにより、送信装置101と受信装置103との間の同期チャンネルの経路(#x→#y)が確立される。

【0071】

次に、送信装置101は、同期チャンネル#xを通して、暗号鍵Kにて暗号化されたAVストリームを送信する(S504)。

【0072】

なお、この時点ではまだ認証要求も認証・鍵交換も行われていない。また、受信装置 103 はまだ暗号鍵 K を得ていない。

【0073】

中継装置 102 は、同期チャンネル # x から上記暗号化 AV ストリームを受信 (S705) すると、ブリッジテーブルを参照して、この AV ストリームは第 2 の IEEE 1394 バス (105) 側に同期チャンネル # y で送信すべきものであると判断し、第 2 の IEEE 1394 バス (105) 上の同期チャンネル # y を通して、タイムスタンプの値などを適当に変更した上で、送信する (S505、S706)。このとき、暗号化された AV ストリームはそのまま送信する。

【0074】

また、これとともに (同時にもしくは相前後して)、第 1 の IEEE 1394 バス (104) から受信された同期パケットの送信ノード ID を参照して、送信者のノード ID が (A, a) であることを認識すると、この ID 情報をブリッジテーブルの第 1 の IEEE 1394 バス側の送信者の欄に登録する (S705)。また、第 2 の IEEE 1394 バス側の送信者の欄は自分自身である。このときのブリッジテーブルの登録内容が図 5 (b) である。

【0075】

次に、受信装置 103 は、同期チャンネル # y を通して、上記暗号化 AV ストリームを受信する。ここで、受信装置 103 は、受信したデータが暗号化されていることを認識し、この暗号化データの送信者との間での認証・鍵交換の必要性を認識する。ここでは、認証・鍵交換のためには、まず、この暗号化データの送信者 (に関する情報) を取得するための手順を行う必要がある。

【0076】

そこで、受信装置 103 は、受信した暗号化データの送信者 (に関する情報) を取得するために、認証問い合わせ packets を中継装置 102 に対して送信する (S506)。

【0077】

この認証問い合わせ packets は、第 2 の IEEE 1394 バス (105) 上の同期チャンネル # y に対してデータを送信しているのがどのノード (あるいはどの

ノードのどのプラグ) であるのかを確認するためのパケットである。また、このパケットには、この暗号化AVデータを受信しているのが、受信装置103であることを示すために、同期チャンネル番号#yの他に、受信装置103のノードID(B, d)と、受信しているプラグであるiPCR[0]の値等も入っている。

【0078】

なお、実際には、この認証問い合わせパケットは、非同期ストリームにて送られるパケットでもよいが、暗号化AVデータの送信ノードIDの値を見て、暗号化AVデータを同期チャンネル#yにて送信しているのが中継装置102であることがわかるため、中継装置102宛の非同期パケットでもよい。

【0079】

この認証問い合わせパケットを受信(S707)した中継装置102は、ブリッジテーブルの認証先の欄に、「同期チャンネル#yを受信しているのは(B, d)のiPCR[0]である」旨を登録する(S708)。このときのブリッジテーブルの登録内容が図5(c)である。

【0080】

さらに、この同期チャンネルを送信しているのが第1のIEEE1394バス上(104)の(A, a)であることをブリッジテーブルを参照することにより確認(S708)し、(A, a)に対して認証問い合わせをフォワードする(S507, S709)。その際は、認証問い合わせパケットにおける同期チャンネル番号は、ブリッジテーブルを参照して、第1のIEEE1394バス(104)上の同期チャンネルに相当する#xに変更しておく。

【0081】

この認証問い合わせパケットを受信した送信装置101は、同期チャンネル#xに対して送信しているのは、ノードIDが(A, a)、プラグがoPCR[0]である旨を、認証応答として返答する(S508)。このとき、認証応答の送信先は、S507における認証問い合わせの送信者であった中継装置102である。

【0082】

この認証応答を受信 (S710) した中継装置 102 は、このパケットを参照して、ブリッジテーブルの第 1 の IEEE1394 側の認証先 ((A, a)、oPCR[0]) を登録する (S710)。このときのブリッジテーブルの登録内容が図 5 (d) である。

【0083】

さらに、第 2 の IEEE1394 バス (105) 上で使用している同期チャンネル番号 #y に変更した上で受信装置 103 に認証応答をフォワードする (S509, S711)。

【0084】

以上の手続きにより、受信装置 103 は、認証・鍵交換を行うべき相手が、送信装置 101 (ノード ID が (A, a)、プラグが oPCR[0]) であることを認識する。この時点で、受信者である受信装置 103 は送信者である送信装置 101 と認証・鍵交換の手続きを行うことができるようになる。

【0085】

続いて、受信装置 103 は、認証要求を送信装置 101 に対して直接送信する (S510)。この認証要求には、送信側の装置のノード ID (A, a) とプラグ oPCR[0]、および受信側の装置のノード ID (B, d) とプラグ iPCR[0] の値が含まれていてもよい。また、この認証要求には受信装置の機器証明 Bcert が含まれていてもよい。

また、送信装置 101 も、認証要求を受信装置 103 に対して直接送信する (S511)。この認証要求にも、送受信側の装置のノード ID とプラグの値が含まれていてもよい。また、この認証要求には送信装置の機器証明 Acert が含まれていてもよい。

【0086】

認証が成立すると、続いて、認証・鍵交換が行われ (S512, S513, S712)、送信装置 101 と受信装置 103 との双方で認証鍵が共有される。次に、送信装置 101 から受信装置 102 に対して、暗号鍵 K を計算するための交換鍵 Kx とシード Nc が送信され (S514)、受信装置 103 は、交換鍵 Kx とシード Nc をもとに暗号鍵 K を計算することができるようになる。

【0087】

これ以降、中継装置102を介して、送信装置101と受信装置103との間で暗号鍵Kによる暗号通信を行うことができる。

【0088】

すなわち、送信装置101が、送信するMPEG映像を、暗号鍵Kを使って、暗号化部205にて暗号化し、これを第1の1394バス(104)の同期チャンネル#xを通して中継装置102に対して送信する。

【0089】

中継装置102は、送信装置101から同期チャンネル#xを通して送られてくる暗号化されたMPEG映像を、ISO信号送受信部404から無線ISO信号送受信部405を通して、無線同期チャンネル#yに送信する。

【0090】

これを受信した受信装置103は、暗号鍵Kの値を使ってMPEG映像の値を復号化する。(暗号が)復号化されたMPEGデータは、MPEGデコード部306にて(MPEG符号が)デコードされる。デコードされたデータは、例えば、ディスプレイ部307にて再生表示される。

【0091】

このように、あるIEEE1394バスと他のIEEE1394バスとの間にブリッジ・ノードが存在するような相互接続の環境においても、エンドーエンドのノード同士(本実施形態では送信装置101と受信装置103)が認証手続きや鍵交換手続きを行うことができ、さらにその内容を中継装置102を含め、その他のノードが知ることはできない仕組みとなっている。また、コンテンツ保護を必要とする実際のMPEG映像等のデータの転送も、コピーが不可能なように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【0092】

なお、認証問い合わせパケットは、IEEE1394のCSR(コマンドステータスレジスタ)空間の特定のアドレス(レジスタ)に、その送信先を指定して

もよいし、AV/Cのセキュリティコマンドの1つとしてこれを定義してもよい。

【0093】

本実施形態においては、PCR（プラグコントロールレジスタ）番号を認証問い合わせに用いることによる例を示したが、PCRの代わりに、サブユニット番号や、AVデータを転送している同期チャンネル番号を用いて、認証問い合わせを行うように構成することも可能である。

【0094】

（第2の実施形態）

次に、第2の実施形態について説明する。

【0095】

本実施形態も、第1の実施形態と同様に、ブリッジ接続されている場合の認証・鍵交換・暗号化データのやり取りについて説明するが、第1の実施形態との相違点は、中継装置も機器証明を持っており、第1のIEEE1394バス上での認証・鍵交換と第2のIEEE1394バス上での認証・鍵交換とをそれぞれ中継装置が終端する点である。ただし、暗号化データ、交換鍵K_xの値、シードN_cの値は中継装置では終端されずそのままフォワードされる。

【0096】

以下では、第1の実施形態と相違する点を中心に説明する。

【0097】

本実施形態のネットワーク構成例は図1と同様である。送信装置101の内部構成例は図2と同様である。受信装置103の内部構成例は図3と同様である。

【0098】

図8に、本実施形態の中継装置（もしくはネットワーク中継装置）102の内部構成例を示す。

【0099】

本実施形態の中継装置102は、第1の実施形態の構成例と同様に、第1のIEEE1394インタフェース（I/F）1101、第2のIEEE1394インタフェース（I/F）1108、第1のAV/Cプロトコル処理部1102、

第2のAV/Cプロトコル処理部 1 1 0 9、第1のコピープロテクション処理部 1 1 0 3、第2のコピープロテクション処理部 1 1 1 0、第1のISO信号送受信部 1 1 0 4、第2のISO信号送受信部 1 1 0 7、ブリッジテーブル部 1 1 0 5、ブリッジ接続処理部 1 1 0 6を有する。

【0 1 0 0】

第1の実施形態との相違点は、各コピープロテクション処理部 1 1 0 3、1 1 1 0内にそれぞれ機器証明 (C c e r t, D c e r t) を持っている点 (もちろんそれに加えて処理アルゴリズムが相違する点) である。

【0 1 0 1】

図9に、本実施形態におけるシーケンス例を示す。

【0 1 0 2】

また、図10に、本実施形態におけるブリッジテーブルの構成例を示す。

【0 1 0 3】

シーケンスの初期において、送信装置 1 0 1 と受信装置 1 0 3 との間、送信装置 1 0 1 と中継装置 1 0 2 との間、および中継装置 1 0 2 と受信装置 1 0 3 との間で、AV/Cコマンド (S 1 2 0 1)、ブリッジ接続コマンド (S 1 2 0 2, S 1 2 0 3)、暗号化AVデータ (S 1 2 0 4, S 1 2 0 5) がやり取りされる点は、第1の実施形態と同様である。また、第1の実施形態と同様のタイミングで、ブリッジテーブルが図10 (a)、図10 (b) というように登録される。その他のS 1 2 0 1 から S 1 2 0 5 までの手順については説明を省略する。

【0 1 0 4】

なお、この時点ではまだ認証要求も認証・鍵交換も行われていない。また、受信装置 1 0 3 はまだ暗号鍵Kを得ていない。

【0 1 0 5】

第1の実施形態と同様に、S 1 2 0 5 におけるAVストリームを受信した受信装置 1 0 3 は、受信したデータが暗号化されていることを認識し、この暗号化データの送信者との間での認証・鍵交換の必要性を認識し、この暗号化データの送信者を突き止めるための手順を行う。このため、認証問い合わせパケットを中継装置に対して送信する (S 1 2 0 6)。実際には、この認証問い合わせパケット

は、非同期ストリームにて送られるパケットでもよいが、暗号化AVデータの送信ノードIDの値を見て、暗号化AVデータを同期チャンネル#yにて送信しているのが中継装置102であることがわかるため、中継装置102宛の非同期パケットでもよい。この認証問い合わせパケットは、第2のIEEE1394バス(105)上の同期チャンネル#yに対してデータを送信しているのが誰なのかを確認するためのパケットである。このパケットには、この暗号化AVデータを受信しているのが、受信装置103であることを示すために、同期チャンネル番号#yの他に、受信装置103のノードID(B, d)と、受信しているプラグであるiPCR[0]の値等も入っている。

【0106】

この認証問い合わせパケットを受信した中継装置102は、ブリッジテーブルの認証先の欄に、「同期チャンネル#yを受信しているのは(B, d)のiPCR[0]である」旨を登録する。さらに、この同期チャンネルを送信しているのが第1のIEEE1394バス上(104)の(A, a)であることをブリッジテーブルを参照することにより確認し、(A, a)に対して認証問い合わせを行うことを認識する。このとき、第1の実施形態のように、中継装置102がこの認証問い合わせをフォワードするのではなく、本実施形態では、あくまで認証問い合わせを行うのは中継装置102であるとして、認証問い合わせを発行する。その際は、同期チャンネル番号は、ブリッジテーブルを参照して、第1のIEEE1394バス(104)上の同期チャンネルに相当する#xとしておくのはもちろん、AVデータを受信している架空のiPCRを含め、認証問い合わせの送信元は中継装置102の架空のiPCRであるとして、認証問い合わせを送信する(S1207)。また、ブリッジテーブルに、この架空のPCRの値を登録する。なお、架空のPCRの番号は予め定められた架空のPCR用の番号の範囲から選択され、架空でない実在のPCRの番号は予め定められた実在のPCR用の番号の範囲から選択されるものとし、ここでは上記の架空のiPCRの番号は一例としてiPCR[100]であるものとする。このときのブリッジテーブルの登録内容が図10(c)である。

【0107】

この認証問い合わせパケットを受信した送信装置 101 は、同期チャネル # x に対して送信しているのはノード ID が (A, a)、プラグが oPCR [0] である旨を認証応答として返答する (S1208)。このとき、認証応答の送信先は、S1207 における認証問い合わせの送信者であった中継装置 102 である。

【0108】

この認証応答を受信した中継装置 102 は、このパケットを参照して、ブリッジテーブルに送信側の認証先 ((A, a)、oPCR [0]) を登録するとともに、先の受信装置 103 からの認証問い合わせ (S1206) に対する返答として、あたかも自分の仮想の oPCR (oPCR [100] とする) が AV データの送信を行っているものとして、認証応答を返す (S1209)。また、ブリッジテーブルに、この架空の PCR の値を登録する。このときのブリッジテーブルの登録内容が図 10 (d) である。

【0109】

以上の手続きにより、受信装置 103 は、認証・鍵交換を行うべき相手が、中継装置 102 (ノード ID が (B, a)、プラグが oPCR [100]) であることを認識する。この時点で、受信装置 103 と中継装置 102 との間および中継装置 102 と送信装置 101 と間でそれぞれ認証・鍵交換の手続きを行うことができるようになる。

【0110】

続いて、受信装置 103 は認証要求を中継装置 102 に対して、中継装置 102 は認証要求を送信装置 101 に対して、それぞれ送信する (S1210, S1215)。S1211 と S1216 についても同様である。このように第 1 の IEEE 1394 バス (104) と第 2 の IEEE 1394 バス (105) とで認証・鍵交換は独立に行われる。これは、受信装置 103 は (その iPCR [0] に対して) 認証すべき相手先が中継装置 102 (の oPCR [100]) であると認識し、送信装置 101 も (その oPCR [0] に対して) 認証すべき相手为中継装置 102 (の iPCR [100]) であると認識しているためである。

【0111】

以降、送信装置 101 と中継装置 102 との間および中継装置 102 と受信装置 103 との間のそれぞれにおいて、認証要求、認証鍵・交換が行われる（S1210～S12313，S1215～S1218）。

【0112】

また、S1214 と S1219 においては、送信装置 101 から中継装置 102 に送られてきた、交換鍵 K_x およびシード N_c の値を、中継装置 102 はそのまま受信装置 103 に対してフォワードする。これによって、送信装置 101 と受信装置 103 との間で暗号鍵 K を共有することが可能となり、受信装置 103 において暗号化 AV ストリームの復号が可能となる。そして、これ以降、第 1 の実施形態と同様に、中継装置 102 を介して、送信装置 101 と受信装置 103 との間で暗号鍵 K による暗号通信を行うことができる。

【0113】

（第 3 の実施形態）

次に、第 3 の実施形態について説明する。

【0114】

図 11 に、本発明を適用するネットワークの全体構成の一例を示す。

【0115】

本実施形態では、第 1 の IEEE1394 バス（2105）と無線 LAN（2107）との間が第 1 の中継装置 2102 により接続され、無線 LAN（2107）と第 2 の IEEE1394 バス（2106）との間が第 2 の中継装置 2103 により接続されている場合に、第 1 の IEEE1394 バス（2105）に接続された送信装置 2101 から第 2 の IEEE1394 バス（2106）に接続された受信装置へ AV データを転送する場合を例にとって説明する。このとき、これまでの実施形態と同様に、著作権保護のためにこれらの AV データ（一例として MPEG 映像データ）には暗号がかけられた上で送信される場合を考える。

【0116】

以下では、これまでの実施形態と相違する点を中心に説明する。

【0117】

本実施形態の送信装置 2101 の内部構成例は基本的には第 1 の実施形態（図

2 参照)と同様である。受信装置 2104 の内部構成例も基本的には第 1 の実施形態 (図 3 参照)と同様である。

【0118】

図 12 に、本実施形態の中継装置 (もしくはネットワーク中継装置) 2105 , 2107 の内部構成を示す。

【0119】

本実施形態の中継装置 (2105, 2107) は、IEEE1394 インタフェース 2201、無線 LAN インタフェース 2210、第 1 の AV/C プロトコル処理部 2202、第 2 の AV/C プロトコル処理部 2206、第 1 のコピープロテクション処理部 2203、第 2 のコピープロテクション処理部 2205、第 1 の ISO 信号送受信部 2207、第 2 の ISO 信号送受信部 2209、AV/C サブユニット代理処理部 2204、パケットフォーマット変換部 2208 を有する。

【0120】

各コピープロテクション処理部 2203, 2205 内にそれぞれ機器証明 (Cert, Dcert) を持つ。

【0121】

パケットフォーマット変換部 2208 は、チャンネル対応テーブルを持つ。図 13 に、第 1 の中継装置 2102 のチャンネル対応テーブルの例を示し、図 14 に、第 2 の中継装置 2103 のチャンネル対応テーブルの例を示す。

【0122】

ここでは、第 2 の中継装置 2103 について主に述べるが、基本的な動作等は第 1 の中継装置 2102 も、第 2 の中継装置 2103 も、同様である (構成自体は同様であるが、一方には送信装置 2101 が接続され、他方には受信装置 2104 が接続されるという相違から、送信装置 2101 から受信装置 2104 へのパケット転送について見たときにパケットの入側または出側が IEEE1394 バス側かまたは無線 LAN 側かという点で IEEE1394 バス側と無線 LAN 側との論理的な機能が入れ替わるところと、また受信装置 2104 に対して受信チャンネル確認を行うか否かというところなどが、動作として異なってくる)。な

お、以下では、本実施形態の中継装置 2102, 2103 については、第 2 の実施形態における中継装置 102 との相違点を中心に説明する。

【0123】

図 15 に、本実施形態における全体のシーケンス例を示す。

【0124】

なお、鍵交換前に行われる暗号化 AV データ転送までのシーケンスにおいて、送信装置 2101 から受信装置 2104 へ制御コマンドが転送される点、送信装置 2101 から中継装置 2102・中継装置 2103 を経て受信装置 2104 までの経路が設定される点については、第 1、第 2 の実施形態と基本的には同様もしくは類似であり、図 15 においてはそれらの手順の説明を省略している。

【0125】

ここで、本実施形態の中継装置 (2102, 2103) は、一方のネットワーク上のサービスやサブユニットなどの構成認識を自動的に行い、これらのサービスやサブユニット等を、あたかも自分自身 (中継装置自身) のサービスあるいはサブユニットであるとして他方のネットワーク上に見せる機能を持ってもよい。本実施形態では、そのような機能を持つものとして説明している。この機能を実現するのが、AV/C サブユニット代理処理部 2210 である。なお、このような機能の詳細については、例えば電子情報通信学会 IN 研究会 98-215 等に開示されている。

【0126】

図 11 の例においては、第 1 の中継装置 2102 が、無線 LAN (2107) 側に対して、送信装置 2101 の代理サービスを行っているものとする。これによって、無線 LAN (2107) 側では、第 1 の中継装置 2102 内の一構成要素として、送信装置 2101 (のサービスやサブユニット等) が認識される。

【0127】

また、第 2 の中継装置 2103 は、第 2 の IEEE 1394 バス (2106) 側に対して、第 1 の中継装置 2102 内の一構成要素である「当該第 1 の中継装置 2102 が提供している送信装置 2101 の代理サービス」の代理サービスを行っているものとする。つまり、第 2 の中継装置 2103 は、第 2 の IEEE 1

394バス(2106)側に対して、送信装置2101の代理サービスを行っている。これによって、第2のIEEE1394バス(2106)側では、第1の中継装置2102内の一構成要素として、送信装置2101(のサービスやサブユニット等)が認識される。

【0128】

また、中継装置2102, 2103では、代理服务を提供している先のネットワーク側からの制御コマンドをそのネットワーク側のAV/Cプロトコル処理部で受信し、このコマンドが実際にはどのサービス/サブユニットに宛てて送出されたものであるかをAV/Cサブユニット代理処理部2204内のテーブルを参照するなどして認識し、代理服务を行っている元のネットワーク側のAV/Cプロトコル処理部を通して、その代理服务を行っているサービス/サブユニット向けのコマンドに変換し、その元のネットワーク側に送出する。

【0129】

さて、受信装置2104は、上記のようにしてあたかも送信装置2101が第2の中継装置2103の一構成要素であるかのごとく認識し、第2の中継装置2103に対して、その実体は送信装置2101であるところの一構成要素に対する制御コマンドを送出する。

【0130】

第2の中継装置2103では、この制御コマンドを、IEEE1394バス側から受信する。ここで、この制御コマンドは、自装置が代理している無線LAN側の第1の中継装置2102の一構成要素(すなわち送信装置2101の代理服务)宛であることが認識される。したがって、該制御パケットを自装置から第1の中継装置2102宛になるように変換して、無線LAN側に送出する。

【0131】

第1の中継装置2102では、この制御コマンドを、無線LAN側から受信する。ここで、この制御コマンドは、自装置が代理しているIEEE1394バス側の送信装置2101宛であることが認識される。したがって、該制御パケットを自装置から送信装置2101宛になるように変換して、IEEE1394バス側に送出する。

【0132】

この制御コマンドと前後して、送信装置2101から受信装置2104へとつながるQOS（通信品質）を保証するための通信パスの設定が行われる。詳細は省略するが、第1のIEEE1394バス（2105）上では同期チャンネル#xが、無線LAN（2107）上では通信帯域が確保されたチャンネル#yが、第2のIEEE1394バス（2106）上では同期チャンネル#zがそれぞれ確保されるものとする。

【0133】

さて、送信装置2101と第1の中継装置2102をつなぐ同期チャンネル#x、第1の中継装置2102と第2の中継装置2103をつなぐ同期チャンネル#y、第2の中継装置2103と受信装置2103をつなぐ同期チャンネル#zが確立された後、送信装置2101から暗号化されたAVストリームが送信され、第1の中継装置2102、第2の中継装置2103を介して、受信装置2104へ転送される（S2301～S2303）。

【0134】

すなわち、送信装置2101から受信装置2104に対して転送される（暗号化された）AVデータは、第1のIEEE1394バス（2105）上の同期チャンネル#xを通して、第1の中継装置2102に到達する。ここで、ISO信号送受信部2207、パケットフォーマット変換部2208、ISO信号送受信部2209等を通して、無線LAN（2107）上のチャンネル#yに送出される。以下、同様に、第2の中継装置2103を経て、第2のIEEE1394バス（2106）上の同期チャンネル#zを通して、受信装置2104に到達する。ここで、各中継装置において、暗号化されたAVデータの復号化処理は特に行われず、暗号化された部分はそのままの形で（タイムスタンプなどの値や、リンクレイヤヘッダ等は書き換えられる可能性がある）転送される。

【0135】

本実施形態では、各中継装置2103内には、これらのチャンネル間の関係を記述するためのチャンネル対応テーブルが用意されるが、この時点では、第2の中継装置2103のチャンネル対応テーブルにおいては、各々の同期チャンネル番号、送

受信の方向、AVデータの送信者（すなわち、図14の上3行）についての情報が記述されている。つまり、認証先は確定しておらず、第2の中継装置2103は、第2のIEEE1394バス（2106）側に出しているフローが、どのノード向けのデータであるかについては、認識していない。第1の中継装置2102のチャンネル対応テーブル（図13）についても同様である。

【0136】

さて、暗号化されたAVデータを受信した受信装置2104は、この暗号化されたAVデータを復号化するために必要な、暗号鍵に関する情報を入手するために、予め定められている通り、そのAVデータの送信ノードに対して認証要求を送信する（S2304）。この例の場合、受信装置2104は、同期チャンネル#zを通して送られてくるAVデータの送信ノードアドレス（CIPヘッダ内にあるフィールド）を参照して、これが第2の中継装置2103から送られてきているものであることを認識し、第2の中継装置2103に対して、認証要求を送信する。

【0137】

ここで、第1の実施形態（IEEE1394上での認証・鍵交換は、AVデータフロー毎あるいはAV/Cのプラグ毎に行われ、同じノード間では複数の暗号鍵をフロー毎あるいはプラグ毎に使用することが可能であるものとした）とは異なり、第2のIEEE1394バス（2106）においては、同じノード間（本例の場合、第2の中継装置2103と受信装置2104との間）では1つの暗号鍵しか定義できないものとする（ただし、同じコピー制御情報のフローについて；例えば、Never Copyのコンテンツについては、異なるプラグで同時に複数のフローがやり取りされていたとしても、用いられる暗号鍵は同一のものである；なお、コピー制御情報は、例えば、「このデータは何回コピー可」、「このデータはコピー不可」等、送られるデータのコピーをどの様に扱うかが記載されている情報である。）。この点は、第1のIEEE1394バス（2105）側についても（送信装置2101と第1の中継装置2102との間でも）同様とする。これに対し、無線LAN（2107）は、第1の実施形態と同様に、同じノード間でフロー毎あるいはプラグ毎に異なる暗号鍵を使うことができるもの

とする。

【0138】

このように、複数の「同一のノード間でやり取りするフローに同一の暗号鍵しか用いることの出来ない」ネットワーク間を、「同一のノード間でやり取りするフロー毎に異なる暗号鍵を用いることが出来る」ネットワークで接続するのは、以下のような理由がある。すなわち、第1のIEEE1394バス(2105)上に2つ以上の送信装置(例えば、第1の送信装置と第2の送信装置)、第2のIEEE1394バス(2106)上に2つ以上の受信装置(例えば、第1の受信装置と第2の受信装置)が存在し、第1の送信装置と第1の受信装置との間および第2の送信装置と第2の受信装置との間でそれぞれ暗号化されたAVデータやり取りがなされるものとする。この場合、両方のIEEE1394バス間に位置する無線LANがもし「異なるフローに異なる暗号鍵を用いることが出来ない」とすると、上記の2つのフローに対して同じ暗号鍵しか用いることが出来ないことになる。しかし、実際にはどの暗号鍵を使うかは個々の送信装置(例えば第1の送信装置と第2の送信装置)がそれぞれ独立に決定することであり、この例で言えば2つの鍵が同一の値になる保証はない。よって、無線LANにおいてフロー毎に鍵が定義できないと、上記2つの暗号化フローを無線LAN上に転送することが不可能となる。反対に、無線LAN(2107)においてフロー毎に鍵が定義できれば、たとえ第1と第2のIEEE1394バス(2105, 2106)が同一ノード間では単一鍵のサポートしか行っていない場合においても、無線LAN(2107)を使った相互接続の環境で、複数の送信装置から出力される複数のフローを同時にやり取りすることが可能となる。

【0139】

さて、これを実現するためには、第2の中継装置2103には工夫が必要である。すなわち、受信装置2104から認証要求を受け取ったとしても、その認証要求には、「どのフローに関する認証要求か」についての情報は記載されておらず、最終的な鍵交換において、どのフローのための鍵を送信しなければいけないかの判断がつかないという問題がある。そこで、受信装置2104からS2304の認証要求を受信した第2の中継装置2103は、この認証要求がどのチャネ

ル（どのプラグ）が提供している暗号化AVフローに対する認証要求であるかの調査を行うべく、受信装置2104に対して、受信チャンネル確認パケットを送信する（S2305）。このパケットは、「あなたはどのチャンネル／プラグで（暗号化AVデータの）受信を行っているか」について、受信装置2104に問い合わせを行うためのパケットである。これに対し、受信装置2104は受信チャンネル（本実施形態の場合は、#z）を応答する（S2306）。

【0140】

この受信チャンネル確認パケットの手続き（S2305，S2306）は、受信装置2104のプラグに関するレジスタを読み取ることにより、受信装置2104がどのチャンネルのデータを受信しているかどうかを第2の中継装置2103が調査することにより、代用してももちろんよい。

【0141】

受信装置2104が受信している同期チャンネル番号（本例では、#z）を得た第2の中継装置2103は、内部のチャンネル間の関係を記述したチャンネル対応テーブルを参照し、「第2のIEEE1394側に同期チャンネル#zにて送信しているのは、無線LAN側ではチャンネル#yであり、無線LAN側にてチャンネル#yに送信しているのは第1の中継装置である」ということを認識する。つまり、第1の中継装置2102（のOPCR[0]）から受信されているフローが、第2のIEEE1394バス（2106）の同期チャンネル#zにフォワードされていることを知る。これを、図14のチャンネル対応テーブル（第2のIEEE1394側の認証先と受信者の欄）に登録する。

【0142】

さて、第1の中継装置2102と第2の中継装置2103との間では、第1の実施形態にて述べたような認証・鍵交換の手続き（認証手続きにおいて、フローやプラグの単位まで指定して、これを行う）がこれと前後して行われる（S2310～S2315）。S2310の際に図14のチャンネル対応テーブルの無線LAN側の受信者の欄に登録され、S2311の際に無線LAN側の認証先の欄に登録される。また、S2310の際に図13のチャンネル対応テーブルの無線LAN側の認証先・受信者の欄に登録され、S2311の際に無線LAN側の自分自

身のプラグ番号が登録される。

【0143】

また、送信装置 2101 と第 1 の中継装置 2102 との間では、これと前後して、ノード間、すなわち第 2 の中継装置 2103 と受信装置 2104 との間と同様の形（ただし、受信チャネルの確認を行う必要はない）で、認証・鍵交換が行われる（S2316～S2319）。S2316 の際に図 13 のチャネル対応テーブルの IEEE1394 側の認証先・受信者の欄が登録される。

【0144】

なお、第 2 の中継装置 2103 と受信装置 2104 との間でも、残りの認証要求と、認証・鍵交換手続きが行われる（S2307～S2309）。

【0145】

第 1 の中継装置 2102 は、第 2 の中継装置 2103 と第 1 の中継装置 2102 との間で行われる認証・鍵交換の手続きが、（第 1 の中継装置 2102 の出力プラグ oPCR[0] が指定されているため、第 1 の中継装置 2102 におけるチャネル間の関係を記述したチャネル対応テーブル（図 13）を参照することにより）、送信装置 2101 と第 1 の中継装置 2102 との間の認証・鍵交換と結びつけばよいことを認識することができる。そのため、第 1 の中継装置 2102 は、送信装置 2101 と第 1 の中継装置 2102 との間で行われる認証・鍵交換の結果、第 1 の中継装置 2102 に通知される交換鍵 K_x とシード N_c の値を、第 2 の中継装置 2103 に対して（出力プラグが第 1 の中継装置 2102 の oPCR[0]、入力プラグが第 2 の中継装置 2103 の iPCR[0] であることを指定して）フォワードすることができる（S2320, S2321）。

【0146】

同様に、第 2 の中継装置 2103 は、第 1 の中継装置 2102 と第 2 の中継装置 2103 との間で行われる認証・鍵交換の結果、第 2 の中継装置 2103 に通知される交換鍵 K_x とシード N_c の値を、第 2 の中継装置 2103 におけるチャネル間の関係を記述したチャネル対応テーブル（図 14）を参照することにより、これらの鍵が第 2 の IEEE1394 バス（2106）側の同期チャネル #z に関するものであり、その受信先が受信装置 2104 であることを認識すること

ができるため、受信装置 2104 に対して（出力プラグが第 2 の中継装置 2103 の oPCR [0]、入力プラグが受信装置 2104 の iPCR [0] であることを指定して）フォワードすることができる（S2321, S2322）。

【0147】

なお、図 14 のチャンネル対応テーブルは、第 2 の IEEE1394 バス（2106）上の同一の同期チャンネル（例えば、#z）について複数の受信者が存在する場合は、その受信装置の数だけ用意する。これにより、各々の受信装置に対して、正確に鍵の値などを通知することが可能となる。

【0148】

上記の点は、第 1 の IEEE1394 バス（2105）上の同一の同期チャンネル（例えば、#x）について複数の送信者が存在する場合における図 13 のチャンネル対応テーブルについても同様である。

【0149】

このようにして、交換鍵 K_x およびシード N_c の値を受け取った受信装置 2104 は、第 1 の実施形態と同様に、暗号鍵の値を計算することができ、暗号化された AV データの復号化を行うことができる。

【0150】

第 1 および第 2 の中継装置（2102, 2103）は、暗号化された AV データを復号化することなく次段のチャンネルにフォワードすることができるため、中継装置を通過する毎に暗号の復号化および再暗号化を行う必要がなくなり、大幅な処理コストの低減を図ることができるようになる。

【0151】

なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0152】

また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0153】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0154】

【発明の効果】

本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図1】

本発明の第1、第2の実施形態に係るネットワークの全体構成の一例を示す図

【図2】

本発明の第1、第2、第3の実施形態に係る送信装置の内部構造の一例を示す図

【図3】

本発明の第1、第2、第3の実施形態に係る受信装置の内部構造の一例を示す図

【図4】

本発明の第1の実施形態に係る中継装置の内部構造の一例を示す図

【図5】

本発明の第1の実施形態に係るブリッジテーブルの一例を示す図

【図6】

本発明の第1の実施形態に係る全体のシーケンスの一例を示す図

【図7】

本発明の第1の実施形態に係る中継装置の動作手順の一例を示すフローチャート

【図8】

本発明の第2の実施形態に係る中継装置の内部構造の一例を示す図

【図9】

本発明の第2の実施形態に係る全体のシーケンスの一例を示す図

【図10】

本発明の第 2 の実施形態に係るブリッジテーブルの一例を示す図

【図 1 1】

本発明の第 3 の実施形態に係るネットワークの全体構成の一例を示す図

【図 1 2】

本発明の第 3 の実施形態に係る第 1、第 2 の中継装置の内部構造の一例を示す図

【図 1 3】

本発明の第 3 の実施形態に係る第 1 の中継装置内のチャンネル対応テーブルの一例を示す図

【図 1 4】

本発明の第 3 の実施形態に係る第 2 の中継装置内のチャンネル対応テーブルの一例を示す図

【図 1 5】

本発明の第 3 の実施形態に係る全体のシーケンスの一例を示す図

【符号の説明】

1 0 1, 2 1 0 1 … 送信装置

1 0 2, 2 1 0 2, 2 1 0 3 … 中継装置

1 0 3, 2 1 0 4 … 受信装置

1 0 4, 1 0 5, 2 1 0 5, 2 1 0 6 … IEEE 1 3 9 4 バス

2 0 1, 3 0 1, 4 0 1, 4 0 8, 1 1 0 1, 1 1 0 8, 2 2 0 1 … IEEE
1 3 9 4 インタフェース

2 0 2, 3 0 2, 4 0 2, 4 0 9, 1 1 0 2, 1 1 0 9, 2 2 0 2, 2 2 0 6
… AV/C プロトコル処理部

2 0 3, 3 0 3, 4 0 3, 4 1 0, 1 1 0 3, 1 1 1 0, 2 2 0 3, 2 2 0 5
… コピープロテクション処理部

2 0 4, 3 0 4, 4 0 4, 4 0 7, 1 1 0 4, 1 1 0 7, 2 2 0 7, 2 2 0 9
… ISO 信号送受信部

2 0 5 … 暗号化部

2 0 6, 3 0 6 … MPEG ストレージ部

305…暗号復号化部

307…ディスプレイ部

405, 1105…ブリッジテーブル部

406, 1106…ブリッジ接続処理部

2107…無線LAN

2204…AV/Cサブユニット代理処理部

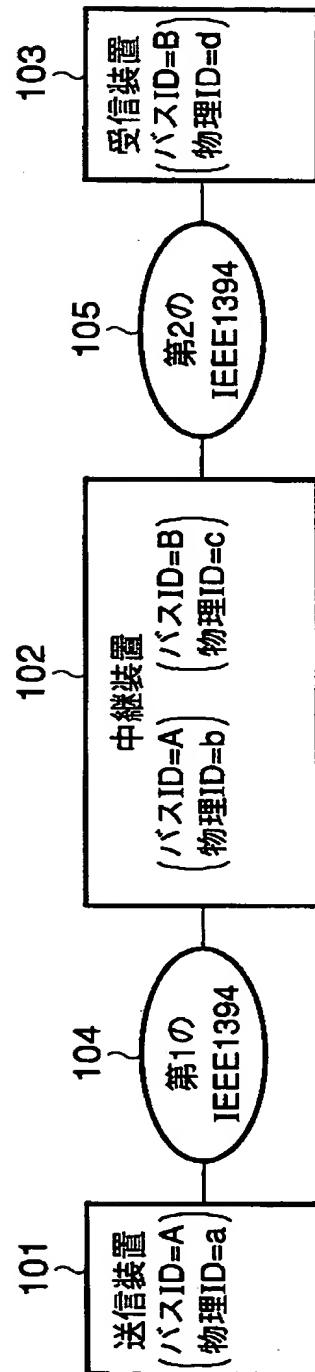
2208…パケットフォーマット変換部

2210…無線LANインタフェース

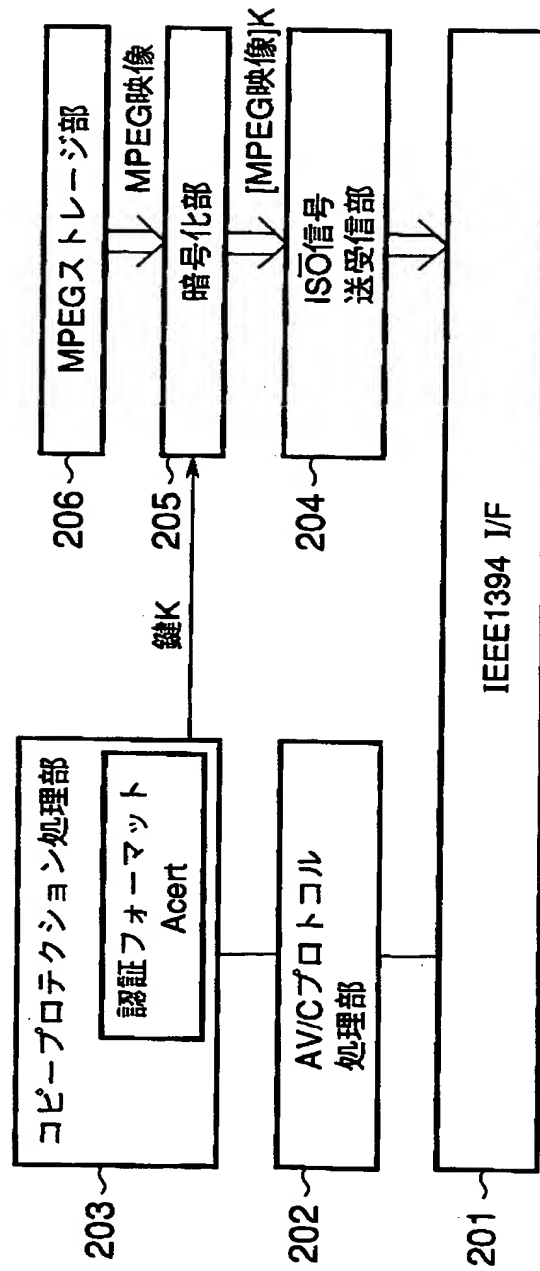
【書類名】

図面

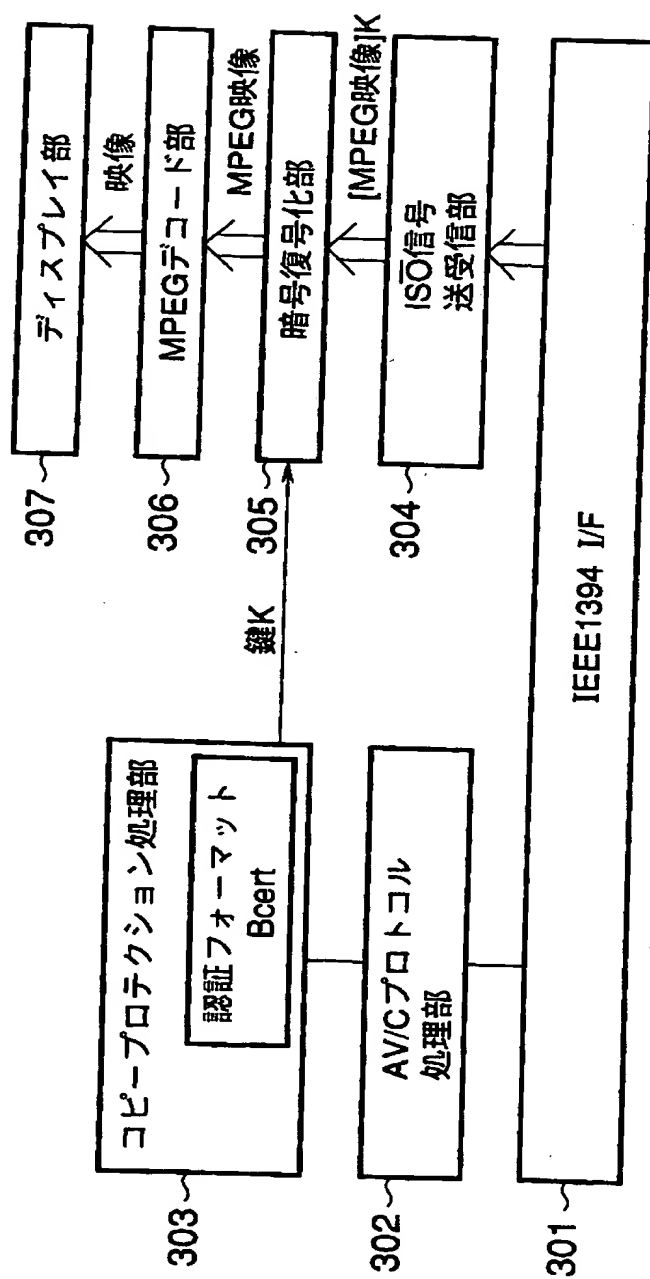
【図 1】



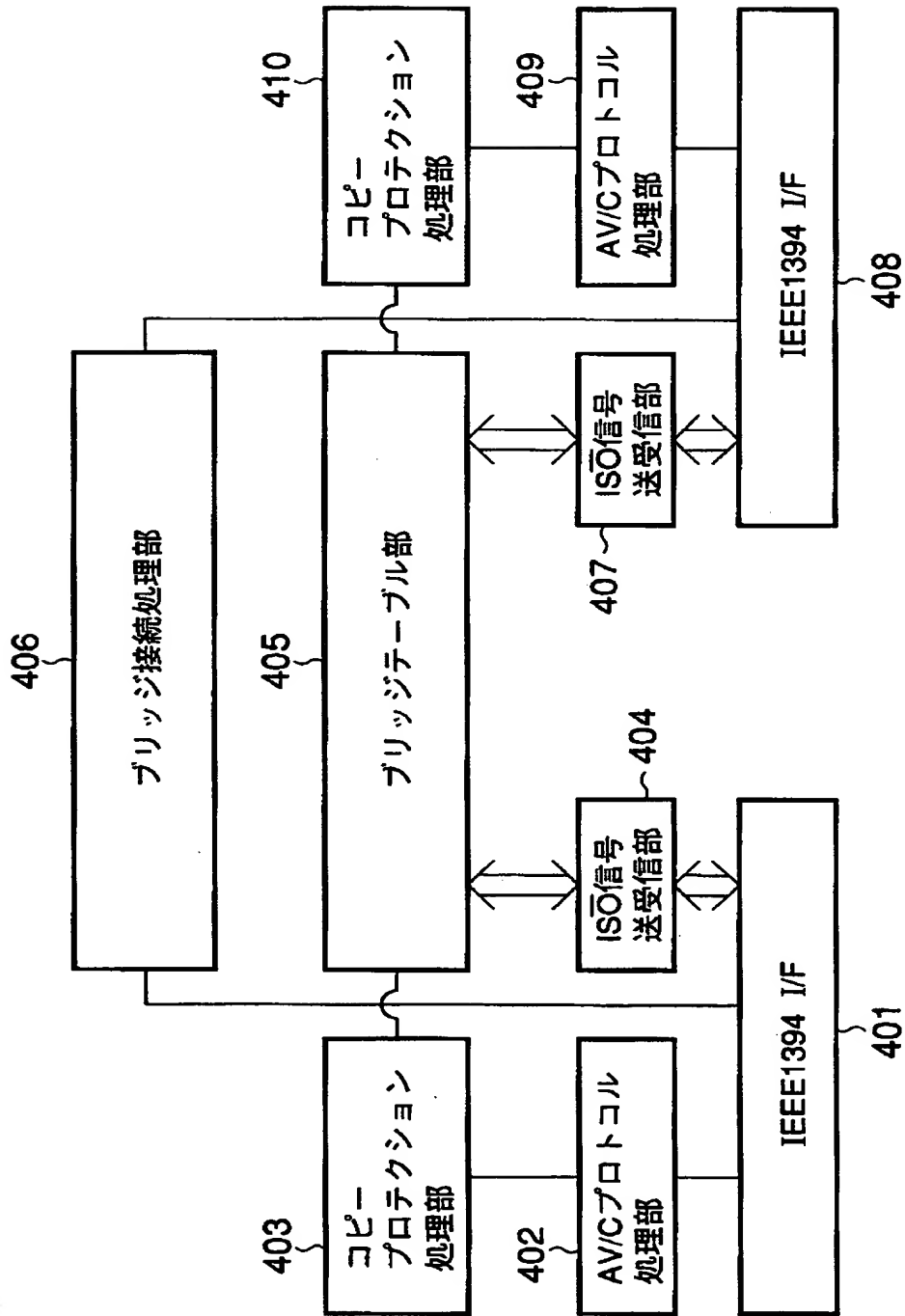
【図 2】



【図 3】



【図 4】



【図 5】

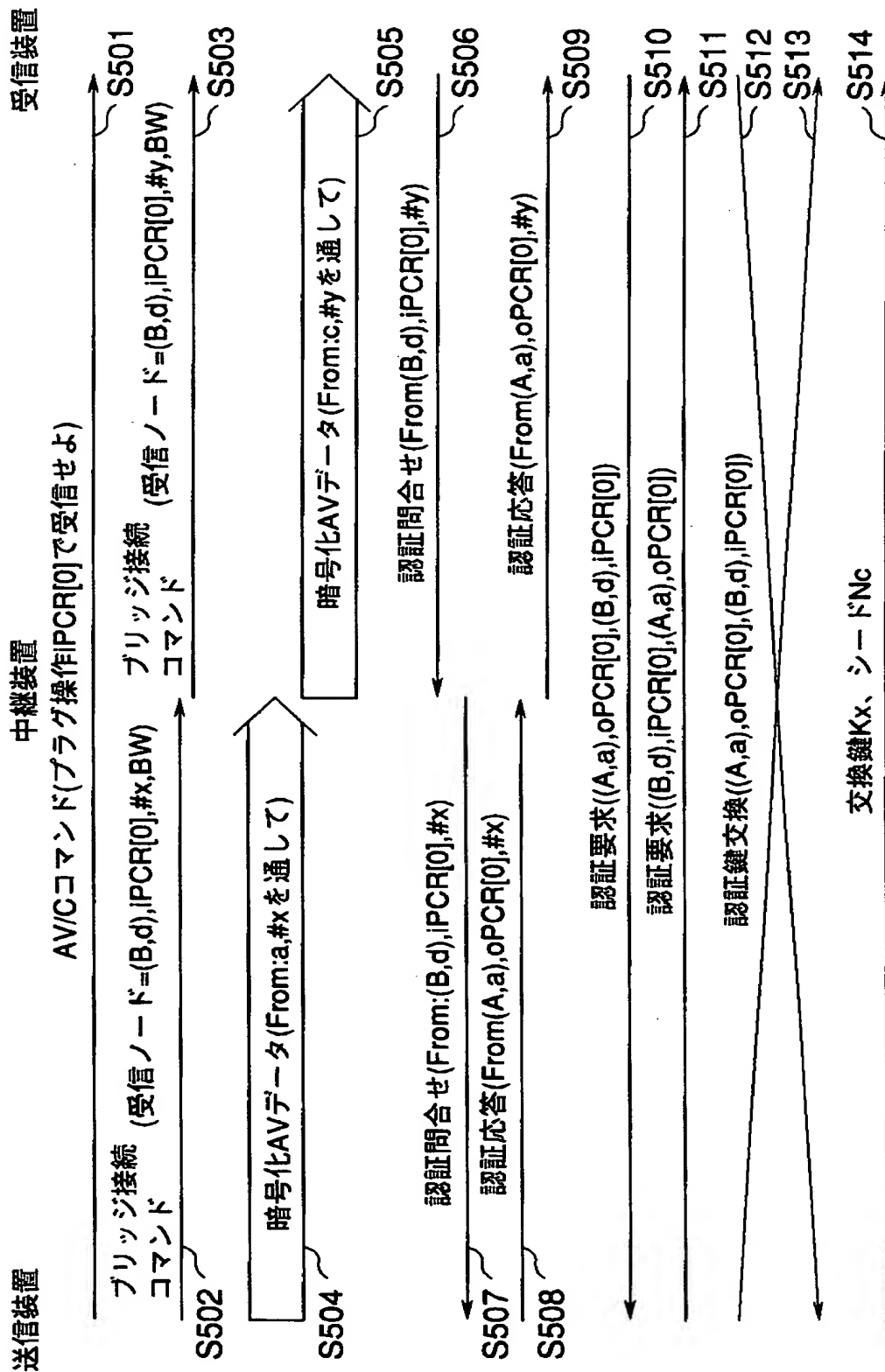
(a)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
		送信者	
		認証先	

(b)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
	(A,a)	送信者	自分自身
		認証先	

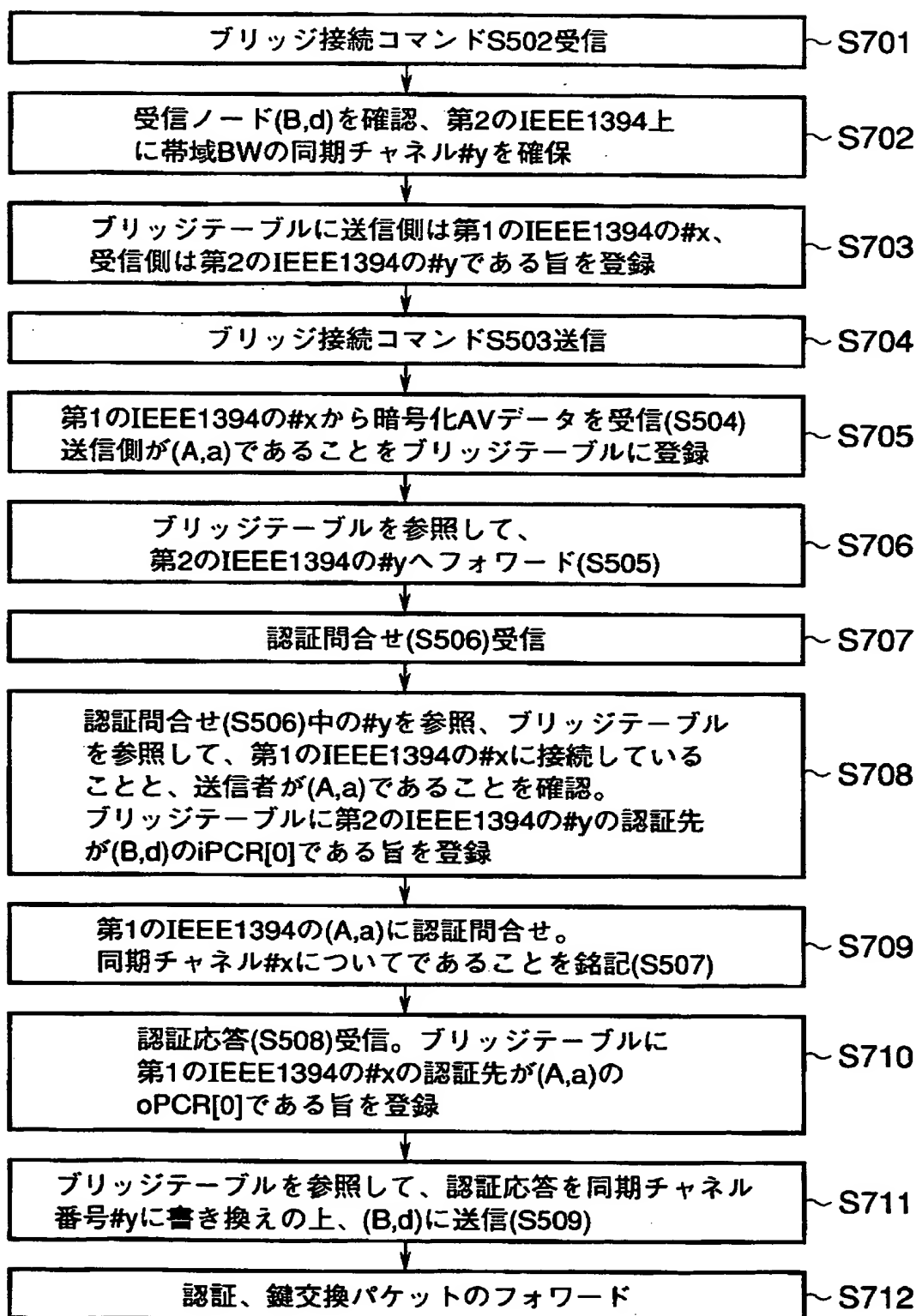
(c)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
	(A,a)	送信者	自分自身
		認証先	(B,d),iPCR[0]

(d)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
	(A,a)	送信者	自分自身
	(A,a),oPCR[0]	認証先	(B,d),iPCR[0]

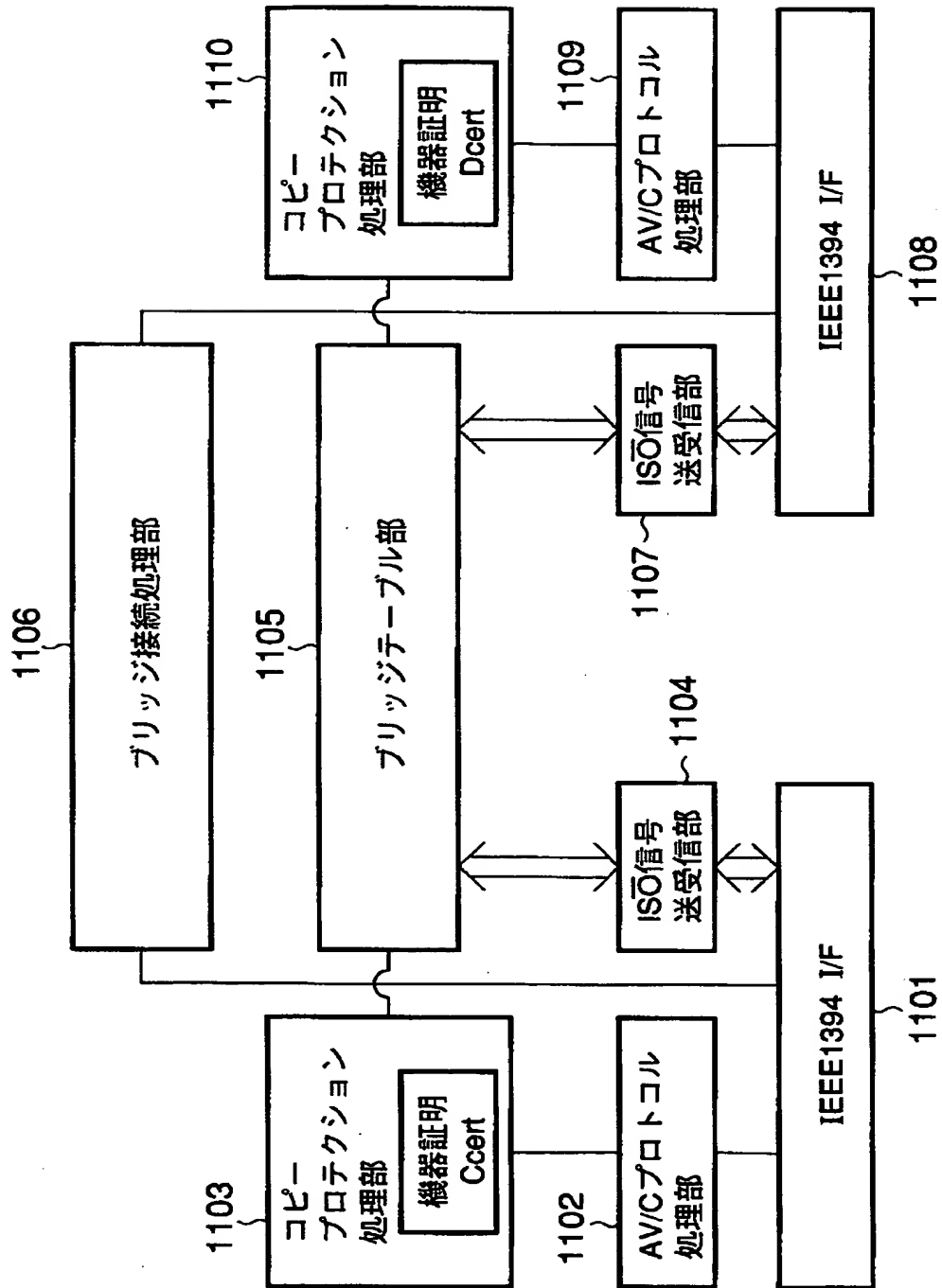
【図 6】



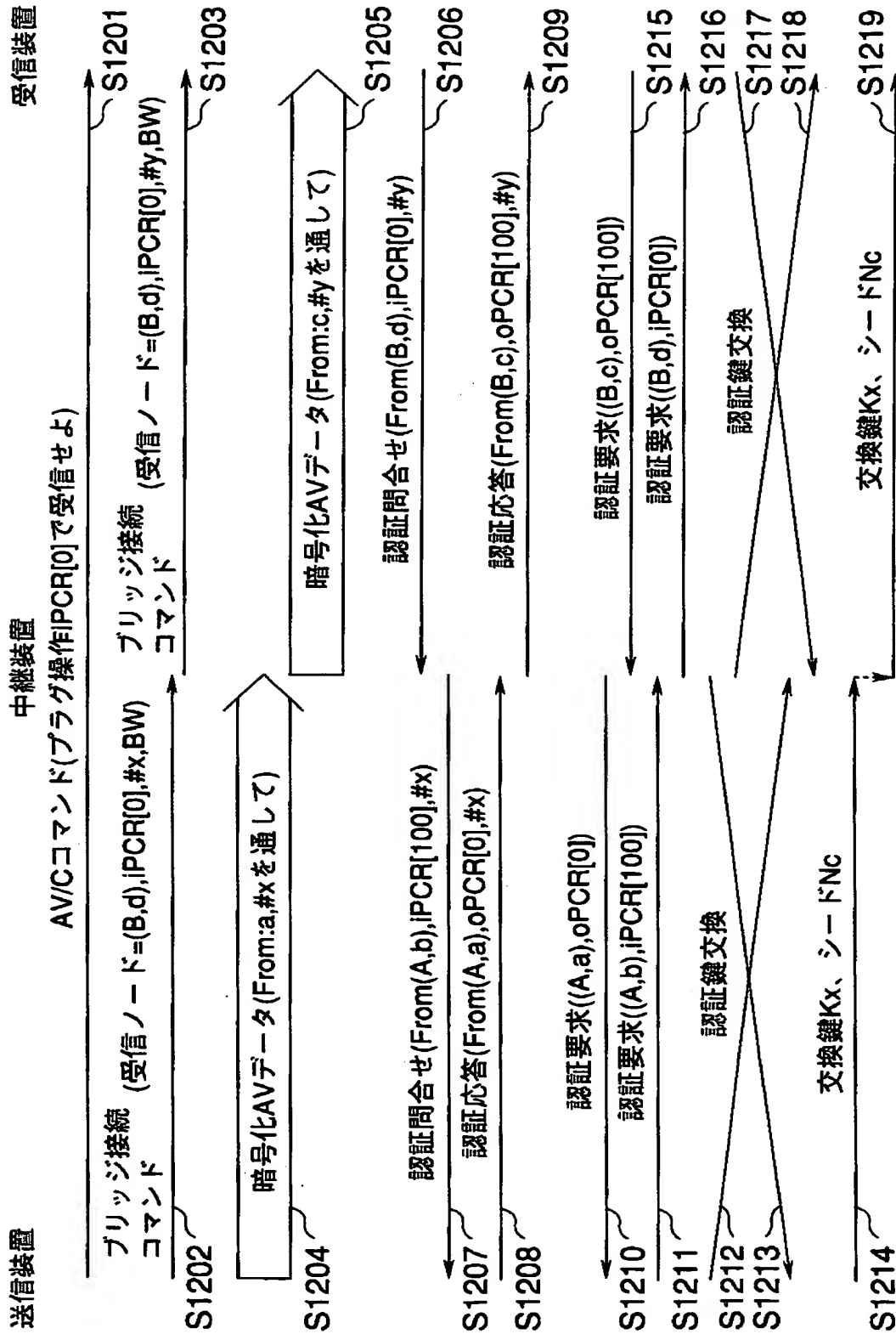
【図 7】



【図 8】



【図 9】



【図 1 0】

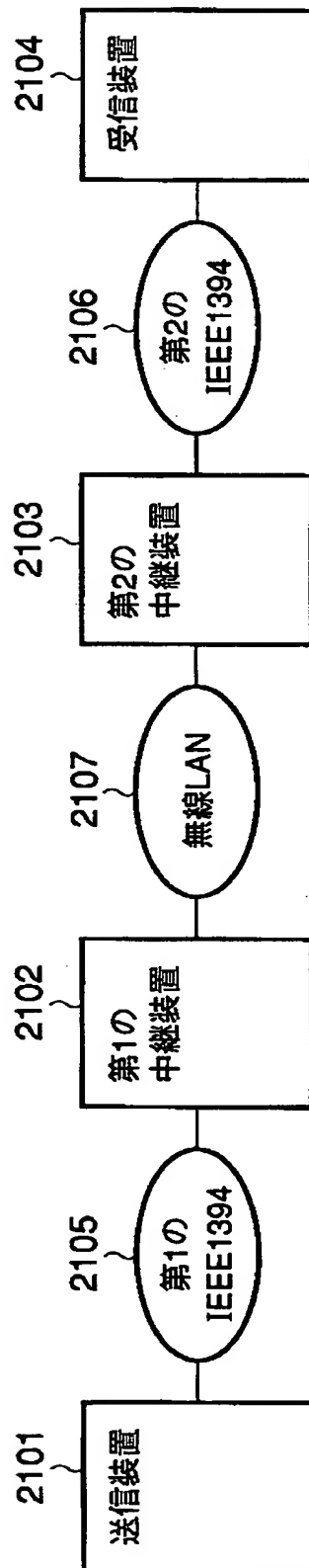
(a)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
		送信者	
		自分自身の仮想的なプラグ	
		認証先	

(b)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
	(A,a)	送信者	自分自身
		自分自身の仮想的なプラグ	
		認証先	

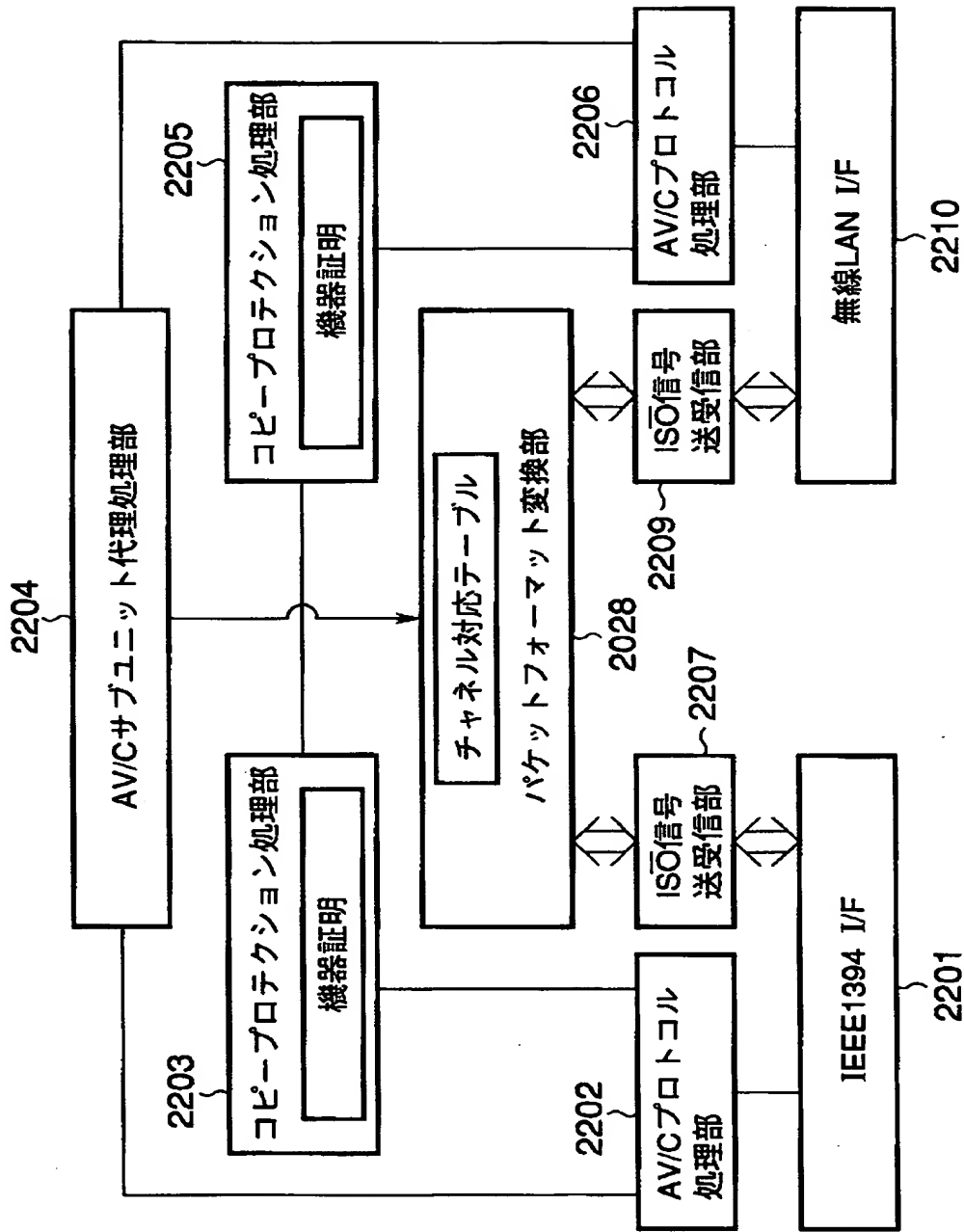
(c)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
	(A,a)	送信者	自分自身
	iPCR[100]	自分自身の仮想的なプラグ	
		認証先	(B,d),iPCR[0]

(d)	第1のIEEE1394側		第2のIEEE1394側
	#x	同期チャネル番号	#y
	送信側	送受信の方向	受信側
	(A,a)	送信者	自分自身
	iPCR[100]	自分自身の仮想的なプラグ	oPCR[100]
	(A,a),oPCR[0]	認証先	(B,d),iPCR[0]

【図 1 1】



【図 1 2】



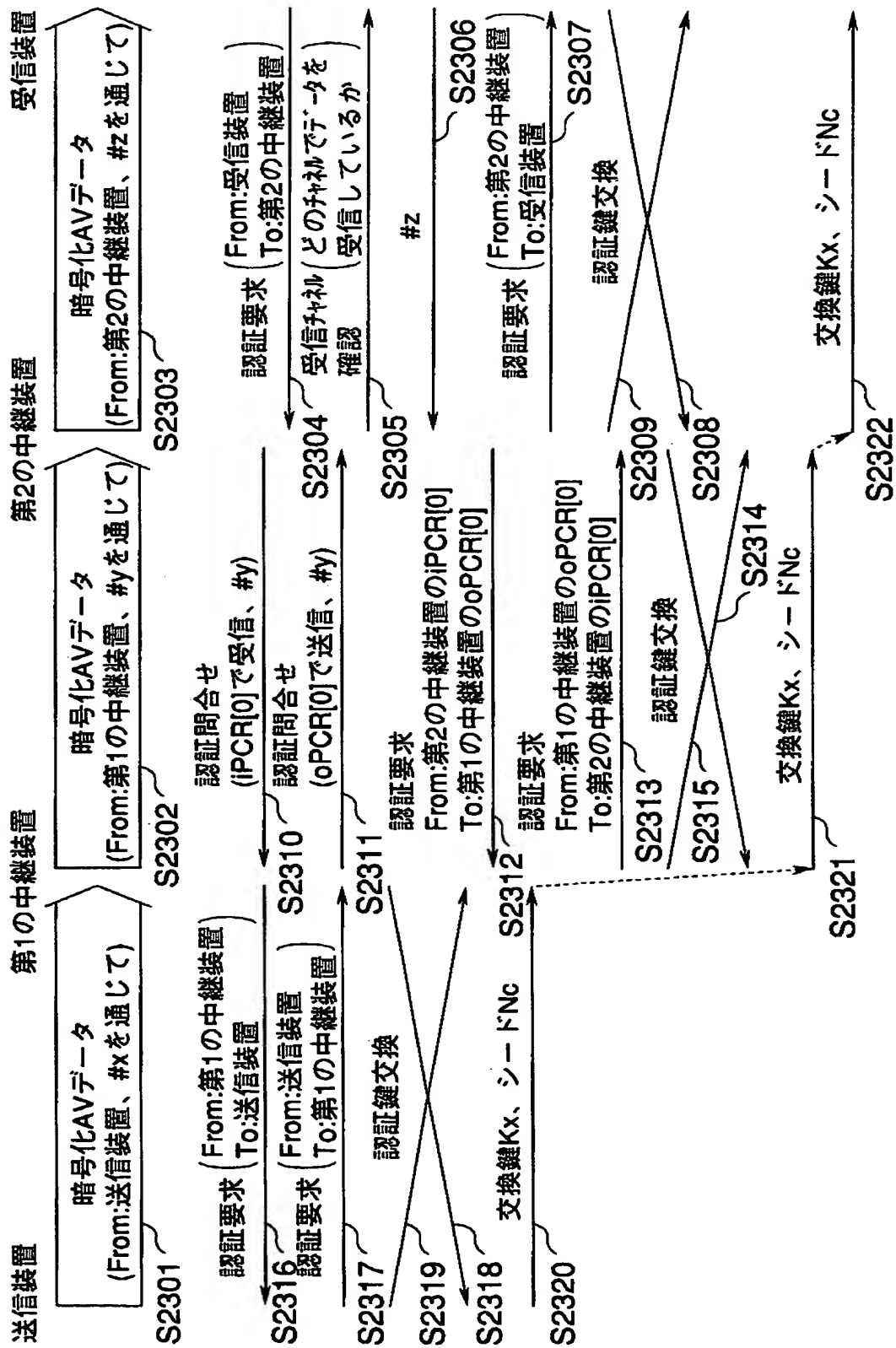
【図 1 3】

第1のIEEE1394側		無線LAN側
#x	同期チャンネル番号	#y
送信側	送受信の方向	受信側
送信装置	送信者	自分自身の oPCR[0]
送信装置	認証先	第2の中継装置の iPCR[0]
自分自身	受信者	第2の中継装置の iPCR[0]

【図 1 4】

無線LAN側		第1のIEEE1394側
#y	同期チャンネル番号	#z
送信側	送受信の方向	受信側
第1の中継装置	送信者	自分自身
第1の中継装置の oPCR[0]	認証先	受信装置
自分自身の iPCR[0]	受信者	受信装置

【図 15】



【書類名】 要約書

【要約】

【課題】 同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とするネットワーク接続装置を提供すること。

【解決手段】 第 1 の IEEE 1394 バス上の送信装置から、同期チャネル # x、ネットワーク接続装置、同期チャネル # y の経路で、第 2 の IEEE 1394 バス上の受信装置へ、暗号化されたデータが転送される。受信装置は、このデータが暗号化されている場合、ネットワーク接続装置にこのデータの送信装置に関する情報の問い合わせを行う。ネットワーク接続装置は、これに応答して、該データの送信装置に関する情報の問い合わせを第 1 の IEEE 1394 バス上で行い、これによって得られた送信装置に関する情報を、受信装置に通知する。受信装置は、受信された前記情報に基づいて、送信装置との間で、直接認証・鍵交換手続きを行う。

【選択図】 図 6

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝